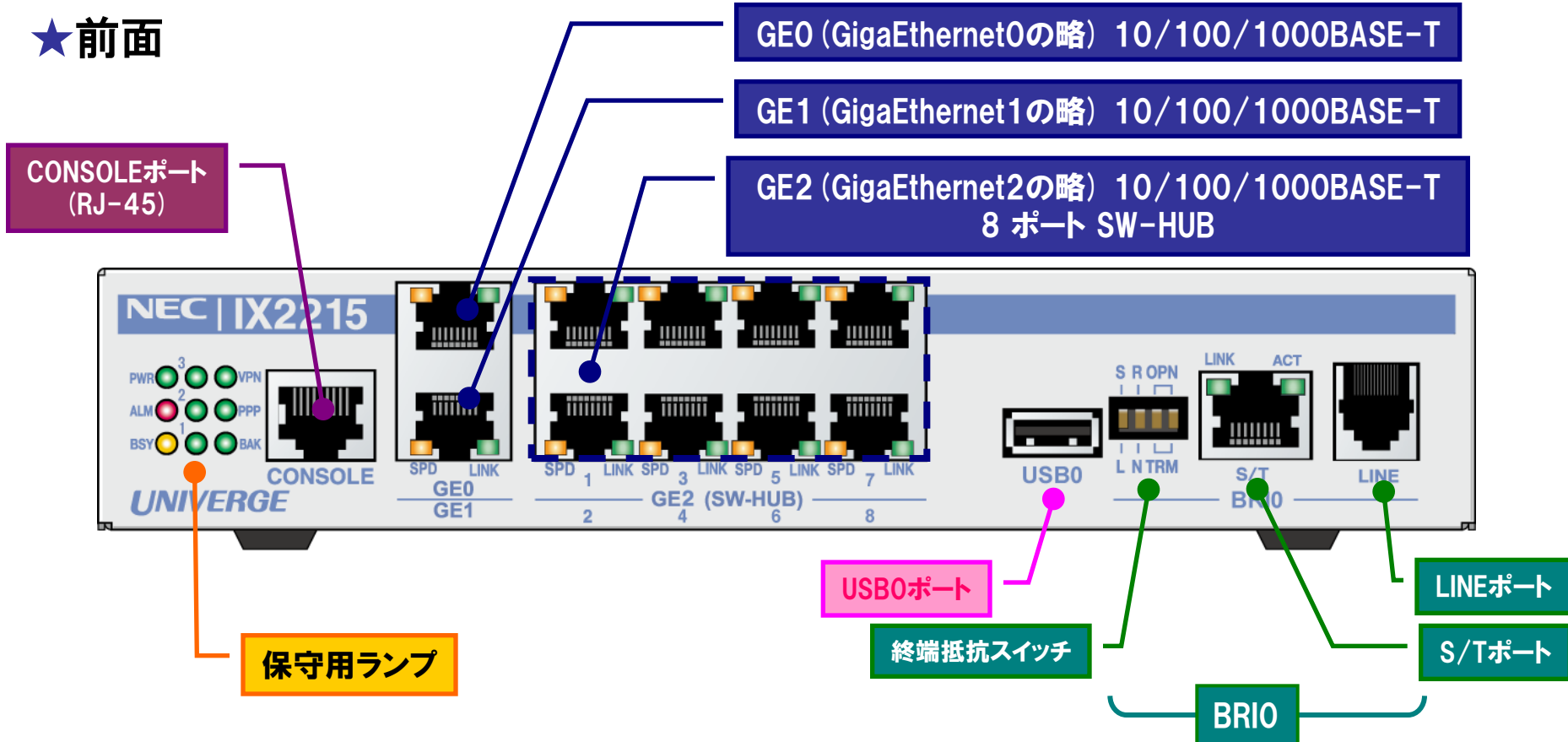
Empowered by Innovation NEC

実機演習資料（初級編）
～UNIVERGE IX2215～

第10.0版（ver.8.10対応）

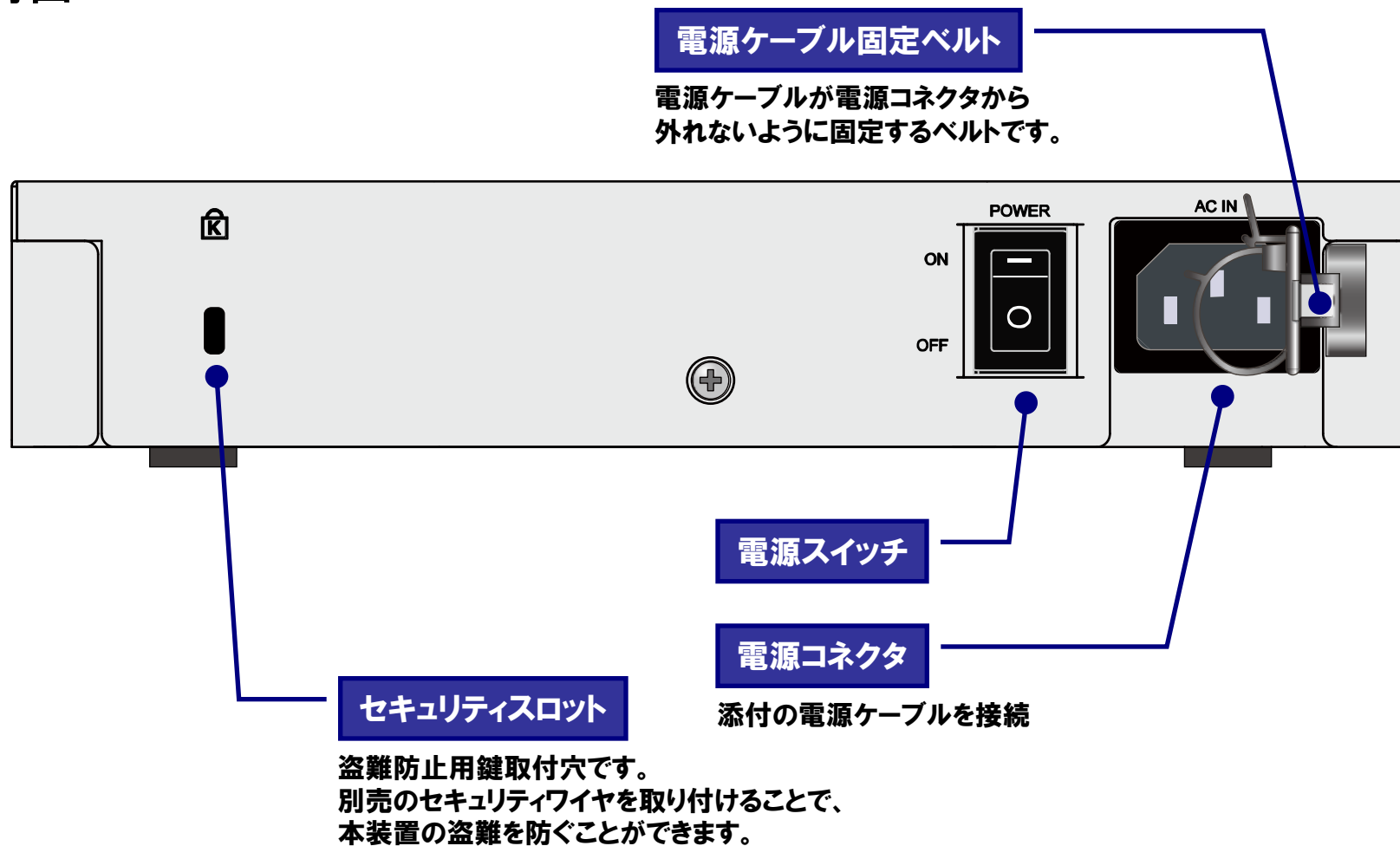
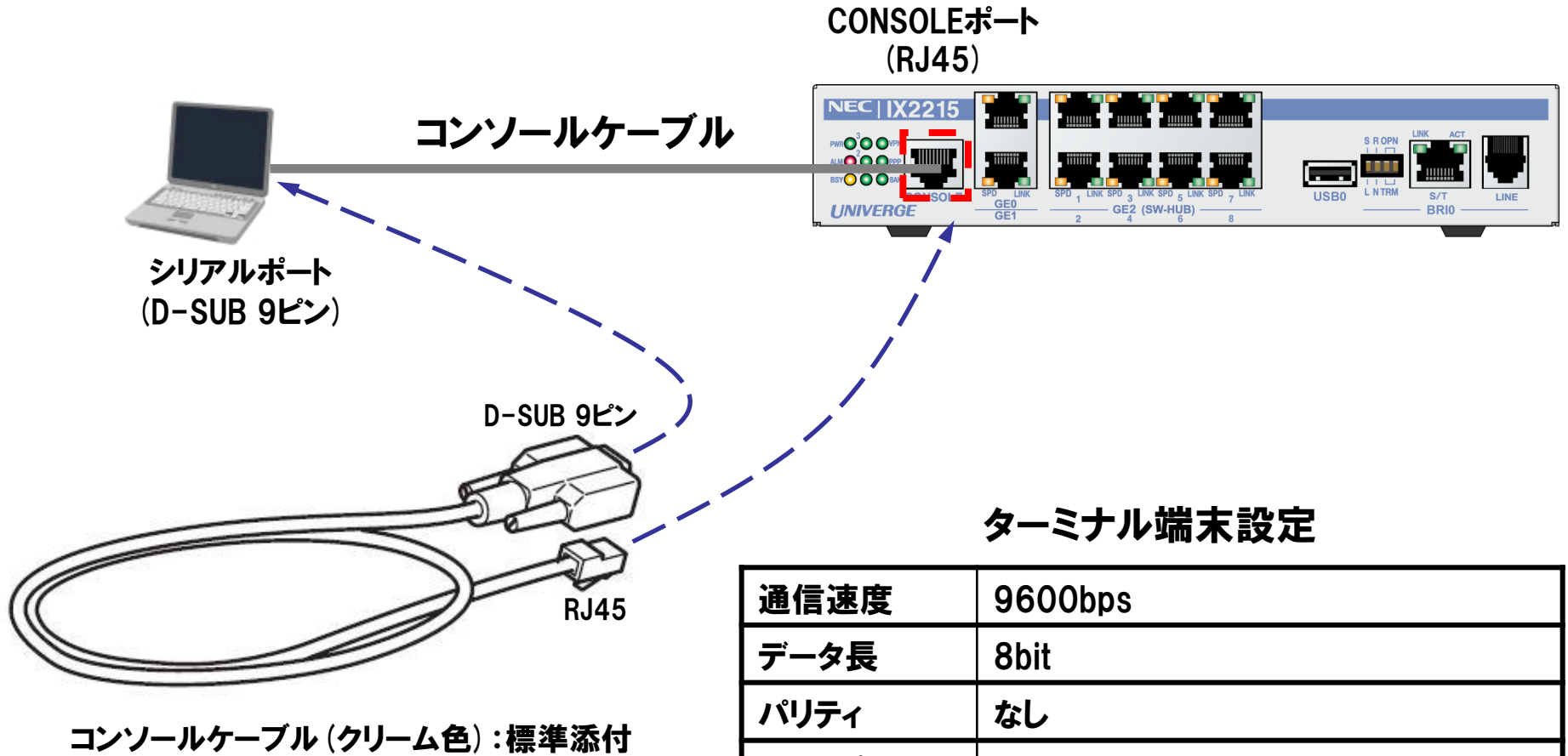
NECインフロンティア株式会社

目次

UNIVERGE IX2215外観図

PWRランプ	電源on時に緑点灯	VPNランプ	IPsecSAが1つ以上確立している時に緑点灯
ALMランプ	ハード異常検出時、及び 温度・電圧異常検出時に赤点灯	PPPランプ	PPPセッションが1つ以上確立しているときに緑点灯 接続中は緑点滅します。
BSYランプ	Flashメモリ書き込み時に橙点滅	BAKランプ	ネットワークモニタ機能により障害を検出すると緑点灯
USB1,2,3ランプ	USB0 ポートに取り付けたデータ通信端末等の状態を緑点灯、点滅、消灯の組み合わせで表示		

UNIVERGE IX2215外観図

コンソール端末の接続

ターミナル端末設定

通信速度	9600bps
データ長	8bit
パリティ	なし
ストップビット	1bit
フロー制御	なし
ターミナルソフトウェア	VT-100準拠通信ソフトウェア (Tera Term、Hyper Terminalなど)

電源の投入(ハードウェア自己診断)

```
NEC Diagnostic Software
Copyright (c) NEC Corporation 2001-2013. All rights reserved.

%DIAG-INFO: Starting System POST(Power On Self Test)

              DRAM TEST 1: Pass
              DRAM TEST 2: Pass
               NVRAM TEST: Pass
                 CPU TEST: Pass
                 PLD TEST: Pass
                 GE0 TEST: Pass
                 GE1 TEST: Pass
       GE2(SW-HUB)1-8 TEST: Pass
                 BRI TEST: Pass
                 USB TEST: Pass
     1.0 VOLTAGE STATUS: 0.987V Pass
     1.5 VOLTAGE STATUS: 1.481V Pass
     2.5 VOLTAGE STATUS: 2.444V Pass
     3.3 VOLTAGE STATUS: 3.251V Pass
     5.0 VOLTAGE STATUS: 4.836V Pass
     TEMPERATURE STATUS: +49.0degC Pass
```

デバイスの診断結果
Passであれば正常な状態である事を表しています。

設置環境の診断結果

▼次ページへ続く

◆自己診断表示例

- 異常検出時は「Fail」と表示されます。
  - ALARMランプ点灯(赤色)
  - NVRAM(不揮発性メモリ)に記録 : show error-logコマンドで表示
  - 「DRAM TEST 1」~「VOLTAGE STATUS」はデバイスの診断結果が表示されます。
    デバイスの診断で Fail 表示があった場合は、修理または交換が必要になります。
    「TEMPERATURE STATUS」で Fail となった場合は、設置環境の温度を見直す必要があります。

ソフトウェアの起動

▼前ページの続き

```
NEC Bootstrap Software
Copyright (c) NEC Corporation 2001-2013. All rights reserved.

%BOOT-INFO: Trying flash load, exec-image [ix2215-ms-8.10.11.ldc].
Loading: ########################################################################## [OK]
```

↑プログラムファイルの起動中

```
Starting at 0x20000

Configuring router subsystems (before IDB proc): done.
Constructing IDB(Interface Database): done.
Configuring router subsystems (after IDB proc): done.
Initializing router subsystems: done.
Starting router subsystems: done.

All router subsystems coming up.
```

<省略>

```
Router#
```

←ルータが正常に起動するとプロンプトが表示されます。

- プログラムファイルの起動中は「#」を連続表示。
  - Ctrl + cを押下するとブートモニタモードに移行

コマンド入力について

■コマンド入力

本装置は、CLI (Command Line Interface:コマンドラインインタフェース)でコマンドを受け付けます。

```
Router# help
```


コマンドは、表示されているプロンプトに続けて、1つまたは複数のコマンドをスペースで区切って入力します。
また、パラメータが必要なコマンドも、コマンドとの間をスペースで区切って入力します。
入力は、1バイト文字(半角)の英数字、記号で行います。
一部のコマンド(ログイン、パスワード等)を除いて、大文字、小文字の区別はありません。

■コマンド入力時のエラーメッセージ

コマンドが間違っていたり、ユーザ権限で認められていないコマンドの場合は、エラーメッセージを出力します。

```
Router# halp Enter
% halp  -- Invalid command.
Router#
```

コンソール操作　便利機能（1）

■コマンド補完機能

「Tab」キー、により、数文字を入力しただけで完全な形のコマンドに補完することができます。
入力した文字列で始まるコマンドが1つだけの場合、Tabキーを押すとそのコマンドの残りの文字列が補完されます。

```
Router# en Tab ──→ Router# enable-config
```

★入力した文字列で始まるコマンドが複数ある場合に Tabキーを押すと、コマンドは補完されません。
入力途中の文字列で始まる補完可能なコマンドが表示されます。

```
Router# e Tab
  enable-config   -- Enter configuration mode
  exit            -- Exit from the router
Router# e
```

★「？」キーでも同様の動作になります。その状態で利用可能なコマンドまたはパラメータの説明が表示されます。

```
Router# e?
  enable-config   -- Enter configuration mode
  exit            -- Exit from the router
Router# e
```

コンソール操作　便利機能(2)

■コマンド省略機能

入力した文字列で始まるコマンドが1つだけの場合、そのまま Enterキーでコマンドを投入することができます。

```
Router# en Enter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

★複数の単語を組み合わせたコマンドの場合も、単語毎の省略入力が可能です。

▼例1 「write memory」コマンド(設定保存)を省略して入力しています。

```
Router(config)# wr m Enter
Building configuration...
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
Router(config)#
```

▼例2 「show running-config」コマンド(設定確認)を省略して入力しています。

```
Router(config)# sh run Enter
Current configuration : 934 bytes

! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 8.10.11, RELEASE SOFTWARE
                    ・
                    ・
                    ・
```

コンソール操作　便利機能(3)

コマンド補完／省略	・[Tab]キーで補完(複数の補完候補がある場合は、その候補を一覧表示) ・他に補完候補の無い文字列は省略入力可能 – Router(config)# write memory → wr mem – Router(config)# show interface → sho int	
コマンドのヘルプ	・[?]キーでヘルプ表示	
コマンドの履歴	・過去に実行したコマンドの履歴を[↑]キー、[↓]キーで表示。 ・履歴保持数：9コマンド	
ショートカットキー	[ctrl] + [p]	1つ前に入力したコマンドを表示
	[ctrl] + [n]	1つ後に入力したコマンドを表示
	[ctrl] + [b]	1文字(カーソルの左)に移動
	[ctrl] + [f]	1文字(カーソルの右)に移動
	[ctrl] + [a]	行の先頭へジャンプ
	[ctrl] + [c]	コマンドラインの内容をキャンセル
	[ctrl] + [e]	行の終わりへジャンプ
	[crtl] + [d]	カーソル位置の文字を1文字削除
	[ctrl] + [k]	カーソル位置から行末まで削除
	[ctrl] + [t]	カーソル位置の文字とその前の文字を入れ替え
	[ctrl] + [z]	オペレーションモードに移動

画面表示

一画面に収まらない行数を表示する場合、表示の途中で「---more---」が表示されます。

```
!
interface GigaEthernet0.0
  no ip address
  shutdown
!
interface GigaEthernet1.0
  no ip address
  shutdown
!
!
--More--
```

←出力結果が多いときは「--More--」で表示が止まります。

- **More表示時の操作**
  - [space] キー：次の数行を表示します。
  - [Enter] キー：1行ずつ表示します。
  - [Q] キー：表示を中止し、プロンプトに戻ります。
  - [/] キー：残りの表示から、指定の文字列検索を行います。

モード移行のイメージ

装置からログアウト
exit
オペレーションモード
Router#
★ルータの電源立ち上げ時のモードで、
Reloadや一部の確認コマンドが実行可能
・enable-config
・configure
exit
コンフィグモード
★ルータ全体に関わる設定や確認など
グローバルコンフィグモード
Router(config)#
interface XXXX
device XXXX
・exit
・configure
・exit
・configure
device XXXX
interface XXXX
インタフェースコンフィグモード
Router(config-XXXX)#
デバイスコンフィグモード
Router(config-XXXX)#
★IP設定(基本インタフェース)
★PPPoE設定(サブインタフェース)
★VLAN設定(サブインタフェース)
★物理的なポートの動作を設定
DuplexやSpeedなど

コンフィグモードへの移行

①オペレーションモードからグローバルコンフィグレーションモードへの移行

コマンド「enable-config」 ※省略「en」

```
Router# enable-config
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

コマンド「configure」 ※省略「c」どのモードからでもグローバルコンフィグレーションモードに移行するコマンドです。

```
Router# configure
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

②グローバルコンフィグレーションモードからオペレーションモードへの移行

コマンド「exit」 ※省略「ex」

```
Router(config)# exit
Router#
```

もしくは、キーボードの [Ctrl] + [z] キーでもオペレーションモードへ移行

```
Router(config)# [Ctrl]+[z] ※表示しません
Router#
```

バージョンの確認

バージョンの表示

```
Router(config)# show version
NEC Portable Internetwork Core Operating System Software
IX Series IX2215 (magellan-sec) Software, Version 8.10.11, RELEASE SOFTWARE ①
Compiled Aug 02-Fri-2013 13:34:44 JST #2 by sw-build, coregen-8.10(11)

ROM: System Bootstrap, Version 3.2
System Diagnostic, Version 3.2
Initialization Program, Version 2.1

System uptime is 0 minute
System woke up by reload, caused by command execution   } ②
System started at Oct 18-Fri-2013 13:56:17 JST          }
System image file is "ix2215-ms-8.10.11.ldc" ③

Processor board ID <0>
IX2215 (P1010E) processor with 262144K bytes of memory. ④
3 GigaEthernet/IEEE 802.3 interfaces   }
1 ISDN Basic Rate interface            } ⑤
1 USB interface                        }
1024K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
```

① ソフトウェアバージョン
② 最近の再起動の要因と、再起動の発生時刻
③ 起動に使用したプログラムファイルのファイル名
④ 装置名
⑤ インタフェース構成

製造番号の表示

製造番号の表示

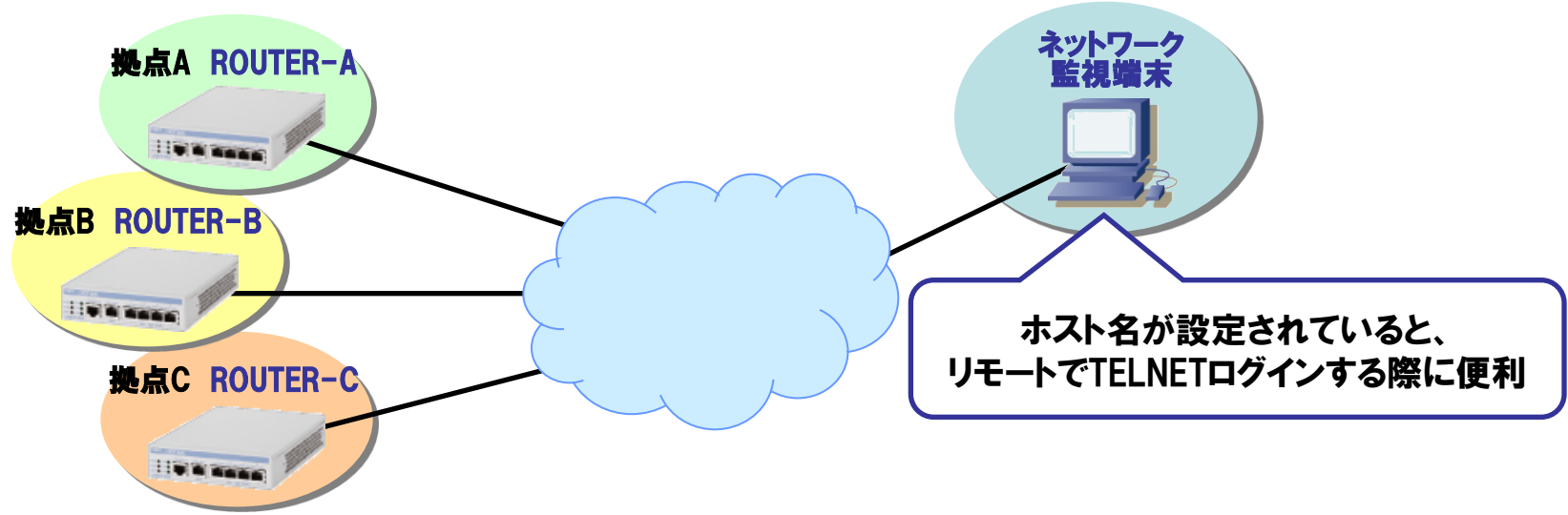
```
Router(config)# show hardware
IX Series IX2215 Hardware Platform

S/N: ********** ①

Processor board:
  Processor board ID <0>
  CPU/DDR3/CSB/LBUS clock frequencies are 792/792/396/99 MHz
  P1010E processor (revision 0x80f90010)
  262144K bytes of main memory
  1024K bytes of non-volatile configuration memory
  32768K bytes of processor flash memory: S29GL256

IPsec accelerator:
  on board security engine(SEC4.4), revision 0x100

Onboard interface unit GigaEthernet0:
  GigaEthernet Transceiver is VSC8552
Onboard interface unit GigaEthernet1:
  GigaEthernet Transceiver is VSC8552
Onboard interface unit GigaEthernet2:
  GigaEthernet Switch with Transceivers is VSC7424
Onboard interface unit BRI0:
  BRI Transceiver is YTD439
```

① S/N番号（装置底面の銘版ラベルに表示している「製造番号」と同じ）

ホスト名の設定

ホスト名の入力

```
Router(config)# hostname ROUTER-A
ROUTER-A(config)#
```

- ホスト名を入力すると、プロンプトの文字列がホスト名になります。
  デフォルト（初期値）は「Router」になっています。

ログイン名の設定

ログイン名の入力

```
ROUTER-A(config)# username admin-user password plain 1 admin-pwd administrator
% User 'admin-user' has been added.
ROUTER-A(config)#
```

・装置のログイン名とパスワードを設定

username [ログイン名] password [パスワードタイプ] [ハッシュ方式] [パスワード] [ログイン権限]

- パスワードタイプ
  - plain : 平文で入力
  - hash : コンフィグ表示時はパスワードをハッシュ化して表示します
- ハッシュ方式
  - 0 : 強度 [普通]
  - 1 : 強度 [強]
- ログイン権限
  - administrator : 全コマンド実行可能
  - operator : 設定情報の変更は実行不可。設定情報の表示、統計情報の表示・クリアは可能
  - monitor : 設定情報の表示・変更は実行不可。統計情報の表示・クリアは可能

・ログイン タイマの設定

terminal timeout □ **←パラメータは「分」で入力します。**

- コンソール無操作時間が指定時間継続したときに、ログインセッションを切断

◎セキュリティ機能

・ログインアカウントの外部サーバ(RADIUS)による管理に可能(AAA機能)

・ログイン／ログアウト時、ログイン失敗時にSNMPトラップの生成が可能

Empowered by Innovation

時刻の設定

時刻の入力

```
ROUTER-A(config)# clock 13 56 00 16 oct 2013
ROUTER-A(config)#
```

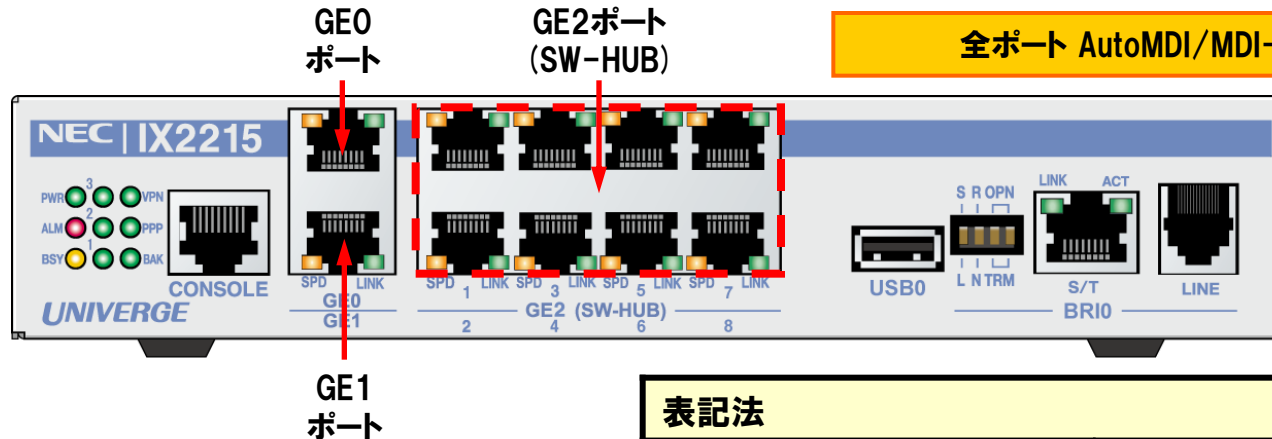
時刻の表示

```
ROUTER-A(config)# show clock
Friday, 18 October 2013 13:57:15 +09 00
ROUTER-A(config)#
```

・IX2215は納入時の時点で時刻情報が設定されています。

◎カレンダー機能

・SNTPクライアント機能に対応しており、NTPサーバ（SNTPサーバ）からのカレンダー情報取得が可能。
・IXルータ自身がSNTPサーバになることも可能。

LANインタフェースの設定(1)

- デバイス設定(ポート単位で有効な設定)
  - speed/duplex
- インタフェース設定
  - IP設定(基本インタフェース)
  - PPPoE設定(サブインタフェース)
  - VLAN設定(サブインタフェース)

表記法	
デバイス設定	device GigaEthernet0 device GigaEthernet1 device GigaEthernet2
基本インタフェース設定 (IP設定)	interface GigaEthernet0.0 interface GigaEthernet1.0 interface GigaEthernet2.0
サブインタフェース設定 (PPPoE/VLAN設定)	interface GigaEthernet0.1 ～ GigaEthernet0.32 interface GigaEthernet1.1 ～ GigaEthernet1.32 interface GigaEthernet2.1 ～ GigaEthernet2.32

▼注意
AutoMDI/MDI-Xは、オートネゴシエーションモードで使用する場合のみ機能します。
通信速度と通信方向をともに固定設定で使用した場合、GE0、GE1はMDI、GE2(SW-HUB)は
MDI-Xとして動作します。 MDI/MDI-Xは、mdi-mdixコマンドにより変更することも可能です。

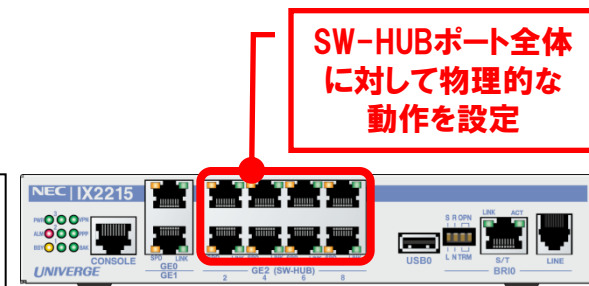
LANインタフェースの設定 (2)

LANポートのモード設定 (デバイスコンフィグモード)

SW-HUBポート全体に対して物理的な動作を設定

★SW-HUBポート全体に対して設定する例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# speed 1000
ROUTER-A(config-GigaEthernet2)# duplex full
```

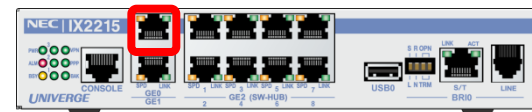
- LANポートのモード設定
  - speed [auto | 1000 | 100 | 10] : オートネゴシエーション (default) 、もしくは10M/100/1000M固定に設定
  - duplex [auto | full | half] : オートネゴシエーション (default) 、もしくは全二重/半二重固定に設定
  - exit で上位モードに復帰

★特定のSW-HUBポートに対して設定する例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# port 1 speed 1000
ROUTER-A(config-GigaEthernet2)# port 8 speed 1000
ROUTER-A(config-GigaEthernet2)# port 1 duplex full
ROUTER-A(config-GigaEthernet2)# port 8 duplex full
```

LANインタフェースの設定(3)

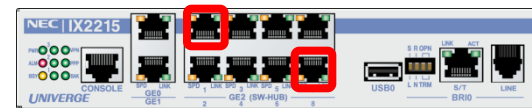
物理ポートのシャットダウン(デバイスコンフィグモード)

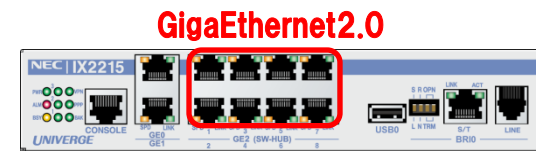
★GigaEthernet0をシャットダウンする例

```
ROUTER-A(config)# device GigaEthernet0
ROUTER-A(config-GigaEthernet0)# shutdown
```

★SW-HUBポート(GigaEthernet2)全体をシャットダウンする例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# shutdown
```

★特定のSW-HUBポートをシャットダウンする例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# port 1 shutdown
ROUTER-A(config-GigaEthernet2)# port 8 shutdown
```

- 使用していないポートをシャットダウンすることで、無駄な消費電力を抑えることができます。
- 使用していないポートの不正な利用を防止することもできます。

LANインタフェースの設定 (4)

GigaEthernet2.0

LANインタフェースの設定 (インタフェースコンフィグモード)

```
ROUTER-A(config)# interface GigaEthernet2.0
ROUTER-A(config-GigaEthernet2.0)# ip address 192.168.□.254/24
ROUTER-A(config-GigaEthernet2.0)# no shutdown
ROUTER-A(config-GigaEthernet2.0)# exit
```

- LANインタフェースの設定
  - IPアドレスの設定
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰

★IPアドレスの第3オクテット目には、**拠点番号(1～10)**を設定してください。

LANインタフェースの設定が完了した方は、IX2215のGE2とPCをLANケーブルで接続後、PCのIPアドレスを変更してください。

【PCのIPアドレス】

IPアドレス
192.168.□.1
サブネットマスク
255.255.255.0
デフォルトゲートウェイ
192.168.□.254

Pingによる疎通の確認

Pingによる疎通の確認（ping 宛先）

PCとIXルータ間の疎通確認を行います。
コマンドプロンプトを起動し、Pingコマンドを実行します。

コマンド プロンプト

例: 拠点1の場合

```
C:¥>ping 192.168.1.254

192.168.1.254 に ping を送信しています 32 バイトのデータ:
192.168.1.254 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.1.254 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.1.254 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.1.254 からの応答: バイト数 =32 時間 <1ms TTL=64

192.168.1.254 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 0ms、平均 = 0ms

C:¥>_
```

本例ではPingを4回送信(Sent)して、応答を4パケット受信(Received)している例です。
パケットロスが0であることを確認します(Lost)。

・応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。

コンフィグの保存

コンフィグの保存

```
ROUTER-A(config)# write memory
Building configuration...
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
ROUTER-A(config)#
```

- write memory
  - running-config(動作コンフィグ)をstartup-config(保存コンフィグ)にコピー
  - コマンド「copy running-config startup-config」と同等

◎参考(その他の保存コマンド)

- startup-configを装置内のファイルシステムに名前を付けて保存
  - copy startup-config *<FILE-NAME>*
- startup-configをTFTPサーバへ送信
  - copy startup-config *<TFTP-SERVER-ADDR>*:<FILE-NAME>
- TFTPサーバからstartup-configをコピー
  - copy *<TFTP-SERVER-ADDR>*:<FILE-NAME> startup-config

コンフィグの削除

コンフィグの削除（設定情報すべての削除）

```
ROUTER-A(config)# erase startup-config
Are you sure you want to erase the startup-configuration? (Yes or [No]): yes
ROUTER-A(config)#
```

- erase startup-config
  - startup-config（保存されているコンフィグ）の削除
- erase startup-configコマンドを実行し、reloadコマンドで装置を再起動することにより、装置を工場出荷時の設定に戻すことができます。

▼実行イメージ

```
ROUTER-A(config)# erase startup-config
Are you sure you want to erase the startup-configuration? (Yes or [No]): yes
ROUTER-A(config)# exit
ROUTER-A# reload
% Warning: current running-configuration is not saved yet.
Notice: The router will be RELOADED. This is to ensure that
        the peripheral devices are properly initialized.
Are you sure you want to reload the router? (Yes or [No]): yes
```

設定の削除

設定の削除（コマンドの削除）

★ホスト名の削除

```
ROUTER-A(config)# no hostname
Router(config)#
```

- show running-configに表示されているコマンドを削除するときは、そのコマンドの頭に「no」を付けて再投入します。

★IPアドレスの削除

```
ROUTER-A(config)# interface GigaEthernet2.0
ROUTER-A(config-GigaEthernet2.0)# no ip address 192.168.1.254/24
ROUTER-A(config-GigaEthernet2.0)#
```

- 特定のモードへ移行しないと削除できないものもあります。
  例えば、IPアドレスのように、インタフェースモードで設定したコマンドは、該当のモードへ移行してから noコマンドで削除します。
  ※アドレスの赤文字部分は省略することも可能です。

設定情報の表示(1)

running-config、startup-configの表示

```
Router(config)# show running-config
Current configuration : 1032 bytes ①

! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 8.10.11, RELEASE SOFTWARE ②
! Compiled Aug 02-Fri-2013 13:34:44 JST #2
! Current time Oct 18-Fri-2013 14:09:15 JST ③

<以降、設定情報を表示>
```

```
Router(config)# show startup-config
Using 1051 out of 1048576 bytes ①

! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 8.10.11, RELEASE SOFTWARE ②
! Compiled Aug 02-Fri-2013 13:34:44 JST #2
! Last updated Oct 18-Fri-2013 14:08:48 JST ③

<以降、設定情報を表示>
```

- **表示内容**
  - show running-config
    - 現在の設定情報と、①コンフィグのサイズ、②バージョン、③このコマンドを実行したときの時刻 を表示
  - show startup-config
    - 保存されている設定情報と、①コンフィグのサイズ、②バージョン、③最後に設定保存した時刻 を表示

設定情報の表示 (2)

```
Router(config)# show running-config
Current configuration : 1032 bytes

! NEC Portable Internetwork Core Operating System
Software
! IX Series IX2215 (magellan-sec) Software, Version
8.10.11, RELEASE SOFTWARE
! Compiled Aug 02-Fri-2013 13:34:44 JST #2
! Current time Oct 18-Fri-2013 14:09:15 JST
!
timezone +09 00
!
username admin-user password hash
9EEC6FA32F3E5f21cCBE8c4F7F214a@ administrator
!
＜省略＞
!
device GigaEthernet0
!
device GigaEthernet1
!
device GigaEthernet2
!
device BRI0
  isdn switch-type hsd128k
!
device USB0
  shutdown
!
```

デバイス情報表示
show running-config device

```
interface GigaEthernet0.0
  no ip address
  shutdown
!
interface GigaEthernet1.0
  no ip address
  shutdown
!
interface GigaEthernet2.0
  ip address 192.168.1.254/24
  no shutdown
!
interface BRI0.0
  encapsulation ppp
  no auto-connect
  no ip address
  shutdown
!
interface USB-Serial0.0
  encapsulation ppp
  no auto-connect
  no ip address
  shutdown
!
interface Loopback0.0
  no ip address
!
interface Null0.0
  no ip address
```

インタフェース情報表示
show running-config interface

show running-config コマンドにパラメータを指定することで、特定の部分のみを表示させることも可能です。

- show running-config device ・・・ デバイス情報表示
- show running-config interface ・・・ インタフェース情報表示
- show running-config access-list ・・・ アクセスリスト表示
- show running-config security ・・・ IPsec/IKE 情報表示

簡易ミス防止

コンフィグチェック

```
Router(config)# check configuration
Check access-list configuration
  [IPSec autokey-map]
    "seclist" on "ipsec1" is not registered
  [IPSec dynamic-map]
    No error
  [route-map]
    No error
  [class-map]
    No error
  [IPv4 filter]
    No error
Check ppp-profile configuration
  Profile name is not bound on BRI0.0
  Profile name is not bound on USB-Serial0.0
```

- 作成したアクセスリストやポリシーが正常に関連付けられているかを確認。
  - IPsec、IPv4フィルタ、ルートマップ、QoSクラスマップ、PPPoEプロファイルのチェックが可能。

テクニカルサポート

テクニカルサポートの表示

```
Router(config)# show tech-support
Calculating configuration memory size...
-------------------- show clock --------------------
Friday, 18 October 2013 14:13:48 +09 00

-------------------- show uptime --------------------
System uptime is 17 minutes
System woke up by reload, caused by command execution

＜省略＞
```

- show tech-support ［no-pausing］
  - 障害発生時の一次解析に必要な統計情報等を一括収集
  - no-pausingをつけると、--more--で区切ることなく、ログを収集することが可能
  - ［Ctrl］＋［c］押下で表示を中断
- terminal length LINES
  - コンソール表示行数の変更（デフォルト 22行）
  - 0に設定すると--more--で区切らずに表示

|補足|　障害発生時、開発側に解析を依頼する際には、一次情報として以下3種類のデータ提出をお願いしています。

1）show tech-support出力データ
2）ネットワーク構成図
3）障害の内容

主な保守・管理コマンド

ping （指定した宛先までの疎通確認）

```
Router# ping 10.10.10.2
```

- pingコマンドはオペレーションモード以下で実行可能 ※グローバルコンフィグレーションモードでも実行可能
- 送信元アドレスの指定、送信サイズなどを1行のコマンドで指定可能
  - ping 192.168.0.254 source 192.168.1.254 size 1000 count 0
    （source 192.168.1.254：送信元アドレス、size 1000：送信サイズ、count 0：送信回数）

traceroute （指定した宛先までの経路情報確認）

```
Router# traceroute 10.10.10.2
```

- tracerouteコマンドはオペレーションモード以下で実行可能 ※グローバルコンフィグレーションモードでも実行可能
- UDPを使用。
- 送信元アドレスの指定などを1行のコマンドで指定可能
  - traceroute 192.168.0.254 source 192.168.1.254
    （source 192.168.1.254：送信元アドレス）

telnetクライアント （telnetクライアント機能の有効化）

```
Router# telnet 10.10.10.2
```

- telnetコマンドはオペレーションモードで実行可能 ※グローバルコンフィグレーションモードでは実行不可能

リモートコンソール (Telnetサーバ)

telnetサーバの有効化

```
Router(config)# telnet-server ip enable
```

- telnetサーバ機能はデフォルト無効。
- telnetサーバのポート番号を変更することも可能。
  - Router(config)# telnet-server ip port 20000
- telnetでの接続を許可するIPアドレスをACLで制限可能
  - Router(config)# telnet-server ip access-list *admin-user-list*

[注意]

- telnetで同時ログイン可能なユーザ数：最大4ユーザ
- ローカルコンソール含め、同時にコンフィグレーションモードに存在できるユーザ数：最大1ユーザ
  - 2ユーザ目がログインを試みた場合、以下エラーメッセージを表示
    Router# enable-config
    % CONFIG process is occupied.
    % You may use `svintr-config' command with administrator privilege.
  - 最初のユーザを追い出す場合はsvintr-configコマンドを実行
    Router# svintr-config
    Enter configuration commands, one per line. End with CNTL/Z.
    Router(config)#

Webコンソール

HTTPサーバ機能の有効化

○ Webコンソールで設定可能なのは IX2105 のみ
IX2025/IX2215/IX3010/IX3110 は表示、メンテナンス機能のみ可能

```
Router(config)# username admin-user password plain 1 admin-pwd administrator
% User 'admin-user' has been added.
Router(config)# http-server ip enable
Router(config)# http-server username admin-user
```

- HTTPサーバ機能はデフォルト無効。
- セキュリティ対策のために、HTTPポート番号(TCP/80)の変更も可能。
  Router(config)# http-server ip port 20000
- HTTPサーバ機能を有効化して、ブラウザのアドレスバーにIPアドレスを指定して接続します。

[例] http://192.168.□.254/

表示例

UNIVERGE IX2215
トップページ - 装置 デバイス Tunnel接続

トップページ

ログインしていません。
各種状態の確認などを行うにはログインする必要があります。

・ログイン
ログイン実行

装置

装置	バージョン	稼働時間	稼働率	メモリ	内部温度	内部電圧	NTP
Router	8.x.x	24 分	14%	18%	+50.0℃	+3.250V	未設定

デバイス

デバイス	接続状態	送信量	受信量
GigaEthernet0	接続されていません	0%	0%
GigaEthernet1	接続されていません	0%	0%
GigaEthernet2	Port1: 全二重 100Mbpsで接続 Port2: 接続されていません Port3: 接続されていません Port4: 接続されていません Port5: 接続されていません	0%	0%

【注意】
ブラウザにプロキシ設定が残っていると、
IXのWebコンソールにアクセスできません。
プロキシを無効化してください。

スーパーリセット

ブートモードでのスーパーリセット

設定したパスワードを忘れてしまい装置にログインできなくなった場合などで、装置の設定を工場出荷時の状態に戻したい場合に、スーパーリセット機能を使用します。

ログの収集(1)

UNIVERGE IXシリーズは、4種類のイベント通知方式をサポートしています。

1. コンソール端末の画面に表示(event-terminal)
2. 内部バッファに蓄積(logging buffered)
3. SYSLOGサーバ(syslog host、IPv4/IPv6に対応)
4. Webブラウザから取得

ログの収集(2)

収集するログの選択	プロトコル・機能単位	・ログを収集するプロトコル・機能と、ロギングレベルの選択 logging subsystem [SUBSYSTEM] [LEVEL] ロギングレベルは下記5段階から選択 少 ←――【ログの量】――→ 多 error, warn, notice, info, debug ・error :エラー状態レベル ・warn :警告状態レベル ・notice :注意レベル ・info :情報レベル ・debug :デバッグレベル	【設定例】 logging subsystem ike debug logging subsystem ospf notice 1)詳細はコマンドのヘルプを参照 2)運用中、debugレベルは使用しないこと Info, debugレベルは、障害解析や現調時に留めること。
	パケットダンプ	・ログを収集するポートを選択 logging packet [DEVICE-NAME] [summary] ・summary : サマリーモードでの出力	【設定例】 logging packet GigaEthernet0 summary 1)運用中には使用しないこと
ログ表示選択	リアルタイム表示	・event-terminal [start/stop]	event-terminalを入力するとログ出力開始、再度入力すると停止
	内部バッファ蓄積表示	・show logging ・show logging statistics [SUBSYSTEM]	
タイムスタンプ	時刻	・logging timestamp timeofday (発生時刻) logging timestamp datetime (発生時刻と年月日)	内部バッファにログを蓄積する場合はdatetimeを推奨
	稼動時間	・logging timestamp uptime (装置稼働時間)	

マニュアルとソフトウェアの情報

ソフトウェアのバージョンアップを行いたい

◆UNIVERGE IXシリーズ 取扱説明書
http://jpn.nec.com/univerge/ix/Manual/index.html

各機能の概要を知りたい

◆機能説明書（機能概要、仕様、諸元）
http://jpn.nec.com/univerge/ix/Manual/index.html

◆FAQ
http://jpn.nec.com/univerge/ix/faq/index.html

設定事例を確認したい

◆設定事例集
http://jpn.nec.com/univerge/ix/Manual/index.html

◆ネットワークサービス毎の事例（フレッツグループなど）
hhttp://jpn.nec.com/univerge/ix/Support/index.html

最新のソフトウェアを入手したい、ログの意味を知りたい

◆ソフトウェアダウンロード（社内イントラネット）
http://ix.nec-i.nec.co.jp/Program/index.html

社外のお客様

貴社ご担当のNEC営業、もしくは、本装置をお買い上げ頂きました販売店にお問い合わせ下さい。

目次

演習1に登場する主な用語

★PPPoE (Point to Point Protocol over Ethernet)
ピーピーピーオーイー

イーサネット上でPPPフレームの配送を可能にするプロトコル。
PPPプロトコルがサポートしている、IPアドレスの払い出しや、ユーザ認証などの技術を
イーサネット回線で利用できるため、ADSLやFTTHなどのブロードバンド回線を使用した
プロバイダ接続で広く使用される。

★NAPT (Network Address Port Translation)
ナプト

IPアドレス変換技術の1つ。
グローバルアドレスとプライベートアドレスを1対1で変換する「NAT」と異なり、更に送信元の
TCP/UDPポート番号も変換することにより、1対N(複数)での変換を実現する。
社内LAN(プライベートネットワーク)から1つのグローバルアドレスを使ってインターネット
アクセスする場合などに使用する。

★Default Route
デフォルトルート

ルーティングテーブル(経路情報)に存在しない宛て先のパケットを受信した際に転送する経路。
主にインターネットアクセスする際にデフォルトルートを設定する。

目的の構成（インターネット接続）

■ プロバイダとPPPoE接続を行い、インターネット上のサーバに接続します。

拠点1

GE2 (SW-HUB)

IX2215

.1 .254

192.168.1.0/24

GE0 10.10.10.□/32

PPPoE

拠点10

IX2215

.1 .254

192.168.10.0/24

GE0 10.10.10.□/32

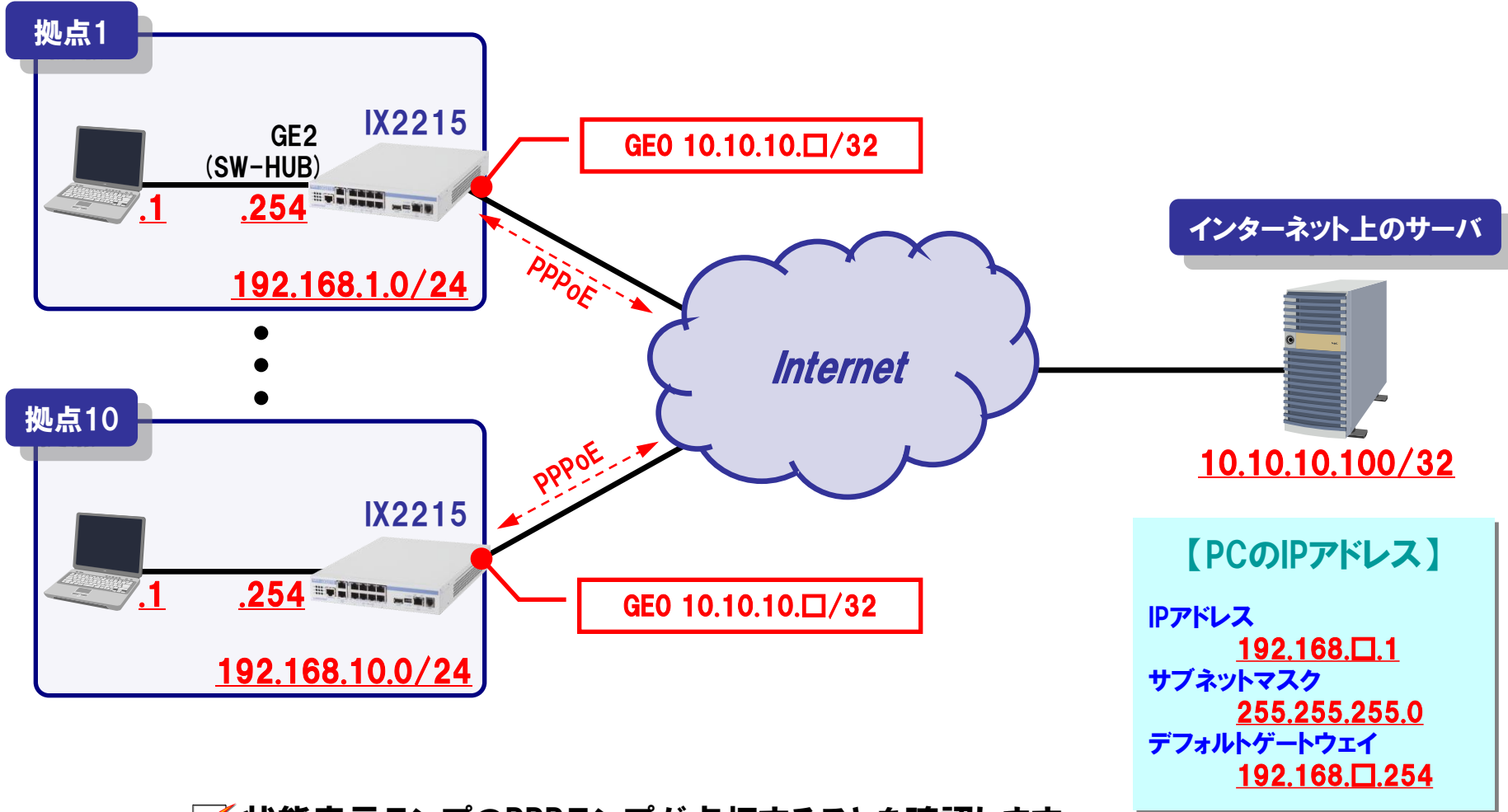
PPPoE

Internet

インターネット上のサーバ

10.10.10.100/32

【PCのIPアドレス】

IPアドレス
192.168.□.1
サブネットマスク
255.255.255.0
デフォルトゲートウェイ
192.168.□.254

- 状態表示ランプのPPPランプが点灯することを確認します。
- 手元のPCからインターネットのサーバ「10.10.10.100」宛にPingが通れば完了です。

LANインタフェースの設定

GigaEthernet2.0

LANインタフェースの設定（インタフェースコンフィグモード）

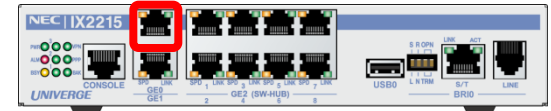
```
Router(config)# interface GigaEthernet2.0
Router(config-GigaEthernet2.0)# ip address 192.168.□.254/24
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)#
```

- LANインタフェースの設定
  - IPアドレスの設定
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰

★IPアドレスの第3オクテット目には、**拠点番号（1～10）**を設定してください。

PPPoEインタフェースの設定

GigaEthernet0.1

PPPoEインタフェースの設定

```
Router(config)# ip ufs-cache enable
Router(config)# ppp profile my-profile
Router(config-ppp-my-profile)# authentication myname test□@test.com
Router(config-ppp-my-profile)# authentication password test□@test.com test□-password
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding my-profile
Router(config-GigaEthernet0.1)# ip address 10.10.10.□/32
Router(config-GigaEthernet0.1)# ip napt enable
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#
```

- PPPプロファイルの設定
  - ppp profile my-profile：ユーザ名／パスワードを設定
  - ppp binding my-profile：PPPoEインタフェースに関連付け
- PPPoEインタフェースの設定
  - IPアドレスの設定
  - NAPTの有効化

★ユーザ名・パスワード、及び、IPアドレスの第4オクテット目には**拠点番号（1～10）**を設定してください。

ルーティング設定

デフォルトルートの設定

```
Router(config)# ip route default GigaEthernet0.1
```

- インターネット接続のためのデフォルトルートを設定
  - GigaEthernet0.1：出力先としてWAN回線に接続するPPPoEインタフェースの名前を指定

ログ収集の設定と設定保存

ログ収集の設定／設定の保存

```
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory
```

・ログの情報を装置の内部バッファに蓄積

Pingによる疎通の確認

Pingによる疎通の確認（ping 宛先）

インターネット上のサーバまでの疎通確認を行います。
コマンドプロンプトを起動し、Pingコマンドを実行します。
コマンド ： ping 10.10.10.100 [Enter]

コマンド プロンプト

```
C:¥>
C:¥>ping 10.10.10.100

10.10.10.100 に ping を送信しています 32 バイトのデータ:
10.10.10.100 からの応答: バイト数 =32 時間 <1ms TTL=62
10.10.10.100 からの応答: バイト数 =32 時間 <1ms TTL=62
10.10.10.100 からの応答: バイト数 =32 時間 <1ms TTL=62
10.10.10.100 からの応答: バイト数 =32 時間 <1ms TTL=62

10.10.10.100 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 0ms、平均 = 0ms

C:¥>
```

本例ではPingを4回送信（Sent）して、応答を4パケット受信（Received）している例です。
パケットロスが0であることを確認します（Lost）。

・応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。

Empowered by Innovation

現在の設定の表示

現在の設定の表示（show running-config）

```
Router(config)# show running-config
Current configuration : 1367 bytes

! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 8.10.11,
RELEASE SOFTWARE
! Compiled Aug 02-Fri-2013 13:34:44 JST #2
! Current time Oct 18-Fri-2013 14:33:12 JST
!
timezone +09 00
!
logging buffered 131072
logging subsystem all warn
logging timestamp datetime
!
ip ufs-cache enable
ip route default GigaEthernet0.1
!
ppp profile my-profile
  authentication myname test1@test.com
  authentication password test1@test.com test1-password
!
device GigaEthernet0
!
device GigaEthernet1
!
device GigaEthernet2
!
device BRI0
  isdn switch-type hsd128k
!
device USB0
  shutdown
!
interface GigaEthernet0.0
  no ip address
  shutdown
!
interface GigaEthernet1.0
  no ip address
  shutdown
!
interface GigaEthernet2.0
  ip address 192.168.1.254/24
  no shutdown
!
interface BRI0.0
  encapsulation ppp
  no auto-connect
  no ip address
  shutdown
!
interface USB-Serial0.0
  encapsulation ppp
  no auto-connect
  no ip address
  shutdown
!
interface GigaEthernet0.1
  encapsulation pppoe
  auto-connect
  ppp binding my-profile
  ip address 10.10.10.1/32
  ip napt enable
  no shutdown
!
interface Loopback0.0
  no ip address
!
interface Null0.0
  no ip address
Router(config)#
```

- 「show running-config」コマンドにより、現在の設定と、ソフトウェアバージョンの確認が可能です。
- 保存した設定を確認するときは「show startup-config」コマンドを使用します。

ログの表示

ログの表示（show logging）

```
Router(config)# show logging
Buffer logging enabled, 131072 bytes, type cyclic
  13 messages (1-13), 1081 bytes logged, 0 messages dropped

Log Buffer (1-13):
2013/10/18 14:29:19   GW.038: User anonymous@ has logged on
2013/10/18 14:29:27  ETH.031: Link status up for port 0, 100M b/s, GigaEthernet0
2013/10/18 14:29:27   IP.021: Interface GigaEthernet0.1, link up
2013/10/18 14:29:27  ETH.031: Link status up for port 1, 100M b/s, GigaEthernet2
2013/10/18 14:29:27   IP.021: Interface GigaEthernet2.0, link up
2013/10/18 14:29:27   IP.021: Interface GigaEthernet2.0, line protocol up
2013/10/18 14:29:27   IP.021: Interface GigaEthernet2.0, up
2013/10/18 14:29:58 PPOE.029: Session start, AccessCT address 00:26:99:db:b4:58, SessionID 1218,
GigaEthernet0.1
2013/10/18 14:29:58  PPP.004: LCP OPENING: state is open, opening upper-link, on GigaEthernet0.1
2013/10/18 14:29:58  PPP.001: NCP OPENING: IPCP state is open, opening upper-link, on GigaEthernet0.1
2013/10/18 14:29:58   IP.021: Interface GigaEthernet0.1, line protocol up
2013/10/18 14:29:58   IP.021: Interface GigaEthernet0.1, up
2013/10/18 14:32:19   GW.079: System woke up by reload, caused by power-on. System started at Oct 18-
Fri-2013 14:29:12 JST
```

- 電源ON後のログ情報を表示します。
- ログの削除には「clear logging」コマンドを使用します。
- インタフェースのlink-up/link-down発生日時などを確認することができます。
- ソフトウェアダウンロードページにある「イベントログリファレンス」では、ログの意味について記載しています。

ルーティングテーブルの表示

ルーティングテーブルの表示（show ip route）

```
Router(config)# show ip route
IP Routing Table - 4 entries, 2 hidden, 2042 frees
Entries: 3 Connected, 1 Static, 0 RIP, 0 OSPF, 0 BGP
Codes: C - Connected, S - Static, R - RIP, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, B - BGP
       * - Candidate default, s - Summary
Timers: Age
S*    0.0.0.0/0 [1/1] is directly connected, GigaEthernet0.1, 0:02:02
      10.0.0.0/8 is subnetted, 1 subnets
C       10.10.10.1/32 [0/1] is directly connected, GigaEthernet0.1, 0:02:02
C     192.168.1.0/24 [0/1] is directly connected, GigaEthernet2.0, 0:13:56
      200.200.200.0/24 is subnetted, 1 subnets
C       200.200.200.1/32 [0/1] is directly connected, GigaEthernet0.1, 0:02:03
```

- 「show ip route」コマンドにより、IPの経路情報テーブルを表示させることが可能です。
- 目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りが無いかを確認する場合に利用します。

PPPoE接続状態の確認(1)

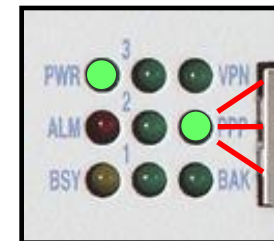
PPPoE接続状態の確認(show ip address)

```
Router(config)# show ip address GigaEthernet0.1
Interface GigaEthernet0.1 is up, line protocol is up
  Internet address is 10.10.10.1/32
  Broadcast address is 255.255.255.255
  Peer address is 200.200.200.1
  Address determined by config
```

- 「show ip address」コマンドにより、PPPoE接続状態の確認が可能です。
- show ip address <I/F NAME>
  - **up**:PPPoEセッション確立
  - **dormant**:PPPoEセッション未確立(ポートup)
    - 網側とPPPoE通信が正常にできていない。
    - PPPのユーザ名/パスワードに誤りがある。
  - **down**:PPPoEセッション未確立(ポートdown)

PPPoEが接続すると装置前面のPPPランプが点灯します。

点灯:接続
消灯:未接続
点滅:ネゴシエーション中

PPPランプが点滅のまま変わらない場合は、認証が失敗している可能性があります。設定したユーザIDとパスワード設定に誤りが無いか見直しをして下さい。

PPPoE接続状態の確認(2)

PPPoE接続の統計確認（show interfaces）

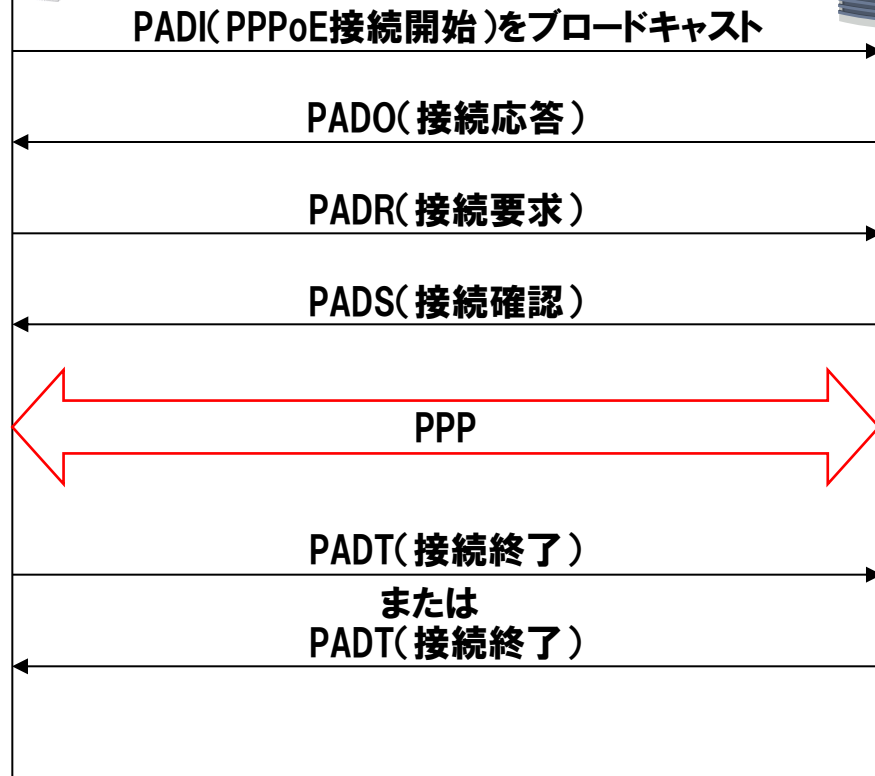
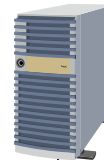
```
Router(config)# show interfaces GigaEthernet0.1 detail
Interface GigaEthernet0.1 is up
:
    CHAP statistics:
      24 packets rcvd, 912 octets
        12 challenges, 0 responses, 4 successes, 8 failures
      12 packets sent, 432 octets
        0 challenges, 12 responses, 0 successes, 0 failures
    PAP statistics:
      0 packets rcvd, 0 octets
        0 auth reqs, 0 auth acks, 0 auth naks
      0 packets sent, 0 octets
        0 auth reqs, 0 auth acks, 0 auth naks
:
  Encapsulation PPPoE:
:
    Statistics:
      PADI: 13 outputs, 0 retries
      PADO: 13 inputs
      PADR: 13 outputs, 0 retries
      PADS: 13 inputs
      PADT: 0 inputs, 11 outputs, 11 timeouts
      10 input discards, 0 output discards
```

認証失敗が無いか確認

- 認証失敗(failures)の数が多い場合、PPPのユーザ名/パスワードの設定に誤りがある可能性があります。

PPPoE再送状況確認

- PADI/PADO/PADR/PADSの送受信数が非常に多い場合、回線が安定していない可能性があります。
- PADIの値のみ増加している場合（網側からPADOの受信が無い）、PPPoE回線に物理的に接続されていない可能性があります。

（参考）PPPoE接続のシーケンス（1）

PPPoEセッションの確立

・PPPoEクライアント側からのPADI送信から4回のメッセージ交換により確立します。

PPPoEセッションの切断

・PPPoEクライアント側もしくはサーバ側からPADT送信により切断が発生します。

（参考）PPPoE接続のシーケンス（2）

PPPoE接続の手順

IX2215

PPPサーバ

LCPフェーズ

Configure-Request （PPPセッション開始）

Configure-Ack

Configure-Request （認証プロトコル要求）

Configure-Ack

認証フェーズ

IPCPフェーズ

Configure-Request （PPPoEサーバのIPアドレス通知）

Configure-Ack

Configure-Request （ルータ側のIPアドレス要求）

Configure-Ack （ルータ側のIPアドレス通知）

Configure-Request

Configure-Ack （PPPoEセッション確立）

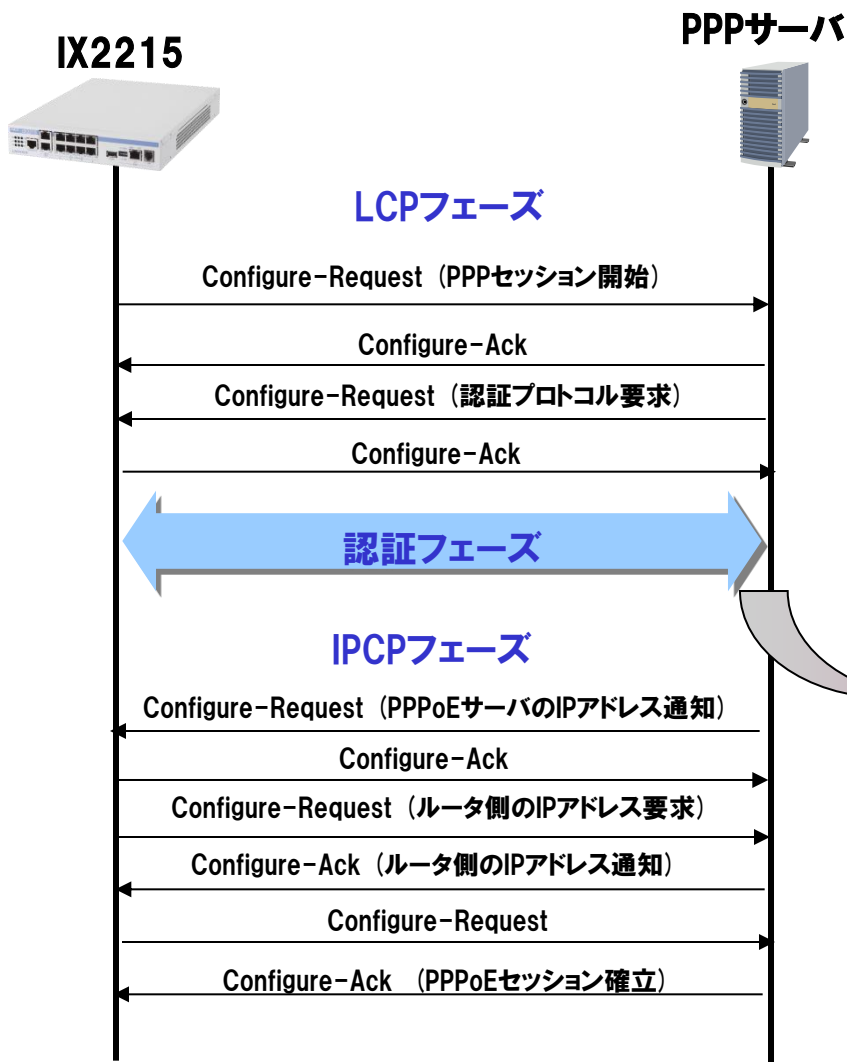
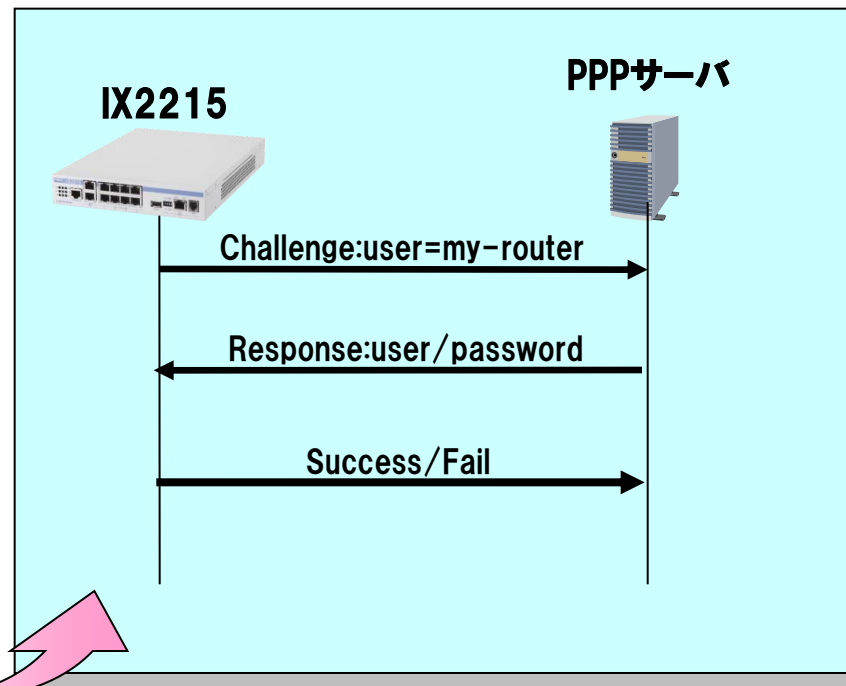
認証フェーズ （CHAPの場合）

IX2215

PPPサーバ

Challenge:user=my-router

Response:user/password

Success/Fail

PPPセッションの確立

- LCPセッションの確立、認証（PAP/CHAP）、IPCPセッションの確立、の3段階で行われます。
- ユーザID/パスワード設定に誤りがある場合、認証の段階でNGになります
- IPアドレスなどIP設定に誤りがある場合、IPCPフェーズでNGになります

NAPTテーブルの表示

NAPTテーブルの表示（show ip napt translation）

```
Router(config)# show ip napt translation
Interface: GigaEthernet0.1
NAPT Cache - 1 entry, 4095 free, 2 peak, 3 create, 0 overflow
Codes: A - ALG, S - Static, Service
  Prot Inside Address:Port   Outside Address:Port   Dest Address:Port     Time
  icmp 192.168.1.1:768       10.10.10.1:768         10.10.10.100:768      60
  tcp  192.168.1.1:1153      10.10.10.1:1153        10.10.10.100:80       58
```

・インターネットへの接続ができない場合に、動的NAPT変換の状態を確認する場合に利用します。
・アドレス変換の情報は一定時間が経過すると消えてしまうため、NAPTテーブルの表示がされない場合は再度、PCからPingを送信してください。

|補足| WANインタフェースでNAPTを有効にしている場合、インターネット側からIX2215のWANアドレスへpingを実行しても、NAPTによりBlock(廃棄)されてしまいます。
NAPT使用時でもIXルータがPingに応答させる場合、PPPoEインタフェースに以下の設定を追加します。

`ip napt static GigaEthernet0.1 1` ← 最後の数字「1」は icmp のプロトコル番号

目次

演習2に登場する主な用語（1）

★**IPsec** (IP Security Protocol)
アイピーセック

IPパケットの暗号と認証を行い、IPレベルでセキュリティ機能を実現するプロトコル。

★**IKE** (Internet Key Exchange)
アイケーイー

インターネット上で鍵の情報を生成、更新する自動鍵交換のプロトコル。
IPsecでは接続する対向装置とお互いに共通の鍵を持ちますが、この鍵の情報をインターネット上で自動的、かつ安全に交換を行わせるためのプロトコル。
IKE自身を安全に暗号化するために、「フェーズ1」、「フェーズ2」の2段階のフェーズが存在する。

★**ISAKMP SA** (Internet Security Association and Key Management Protocol SA)
アイサカンプ・エスエー

IKE自身のメッセージ交換を安全に行わせるために作成される制御用のSAのこと。

★**IPsec SA** (IP Security Protocol Security Association)
アイピーセック・エスエー

IPsecで接続した際のセキュリティを確保する単一方向のコネクション。
暗号、認証のアルゴリズムやライフタイム、事前共有鍵、SPI値（SAの識別子）などを管理する。

★**事前共有鍵** (Pre Shared Key)

IPsec接続する装置間で、通信の暗号化と複合化に使用する秘密鍵を生成する素材となる文字列。

演習2に登場する主な用語(2)

★ライフタイム(Lifetime)

SAの有効時間。秘密鍵の情報を定期的に更新するための時間。
定期的に秘密鍵の情報を更新することで、秘密鍵の情報が解読されたときの被害を最小限に抑えることができる。

★ピアアドレス(Peer Address)

IPsec接続する対向装置(相手側)のアドレス。

★Local ID／Remote ID
ローカルアイディー／リモートアイディー

SAを確立するピアと相互認証を行うためのID情報。

★MTU (Maximum Transmission Unit)
エムティーユー

インタフェースで1回の転送に送信可能なデータの最大サイズ。
MTUの値より大きなパケットの送信が必要な場合は、パケットの分割処理(フラグメント)が発生し、ルータのパフォーマンスに影響する。

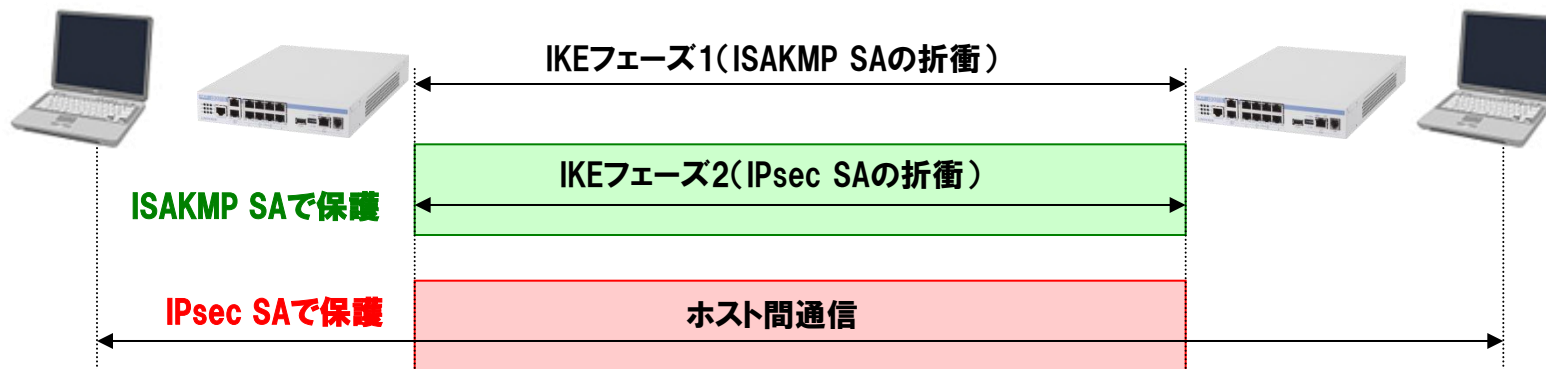
★MSS (Maximum Segment Size)
エムエスエス

TCPで通信を行なう際に指定するデータの送信単位(セグメント)の最大値。
MTUからTCPヘッダーとIPヘッダーの合計値(40 Bytes)を差し引いた値。

IPsecの特長

- IPsec : IP Security Protocol
  - インターネット上を流れる**IPパケットにセキュリティを適用**することができるプロトコル。
  - **データの暗号化**と**メッセージ認証**による盗聴・改ざんの検出
  - データの送信者が正当な相手であることの認証（**相手認証**）
  - パケットのカプセル化による、**パケット送受信者の隠蔽**
  - **VPN(トンネリング)**の構築が可能

IKE（自動鍵）によるIPsecSAの確立

- IKEのプロトコル動作
  - フェーズ1：ISAKMP SAの折衝を行う（メインモード、アグレッシブモード）
    - ・ISAKMP SAは、IPsec SAで使用するパラメータの折衝を保護する目的で使用されます。
  - フェーズ2：IPsec SAの折衝を行う（クイックモード）
    - ・実際に通信を暗号化／認証するための鍵を作成します。

ブロードバンド回線を使用したVPN

ADSLやFTTHなどのブロードバンド回線を使用して、安価で高速なインターネットVPNを構築することが可能です。

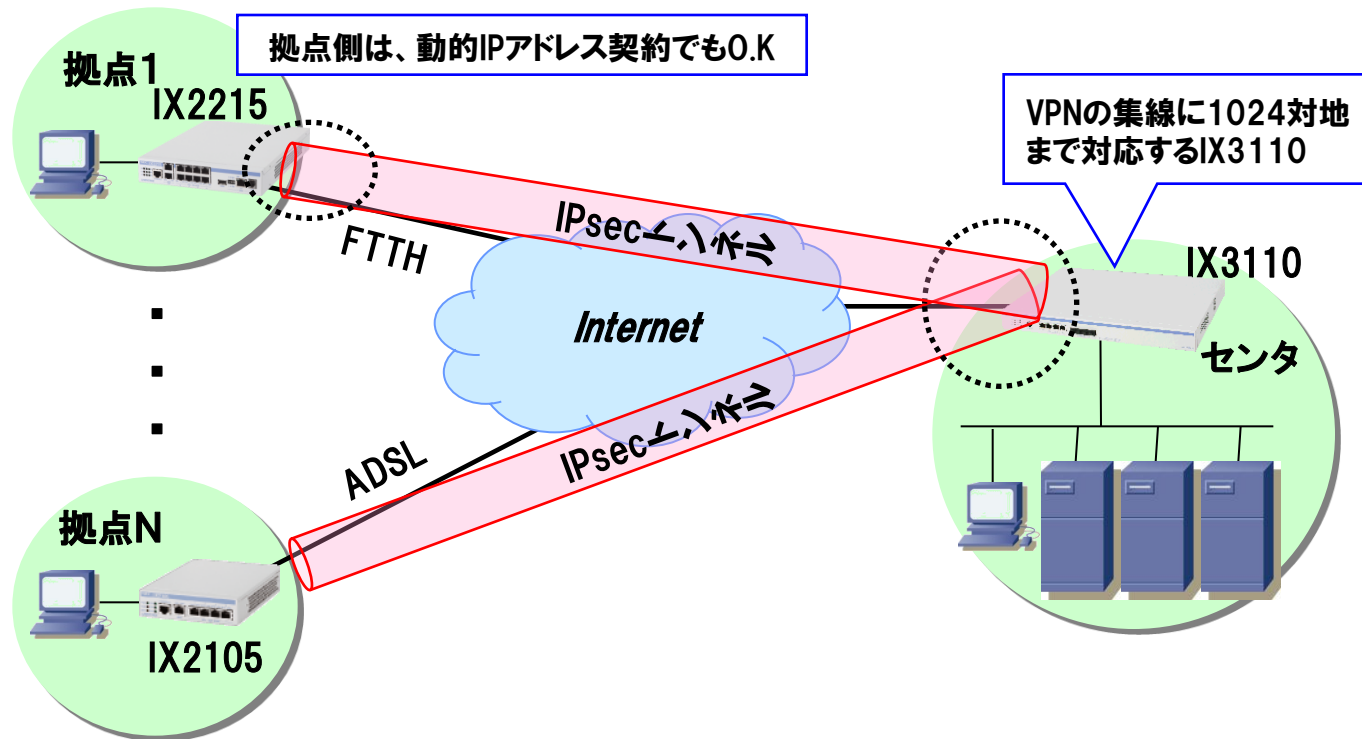
VPN規模に応じたラインナップ

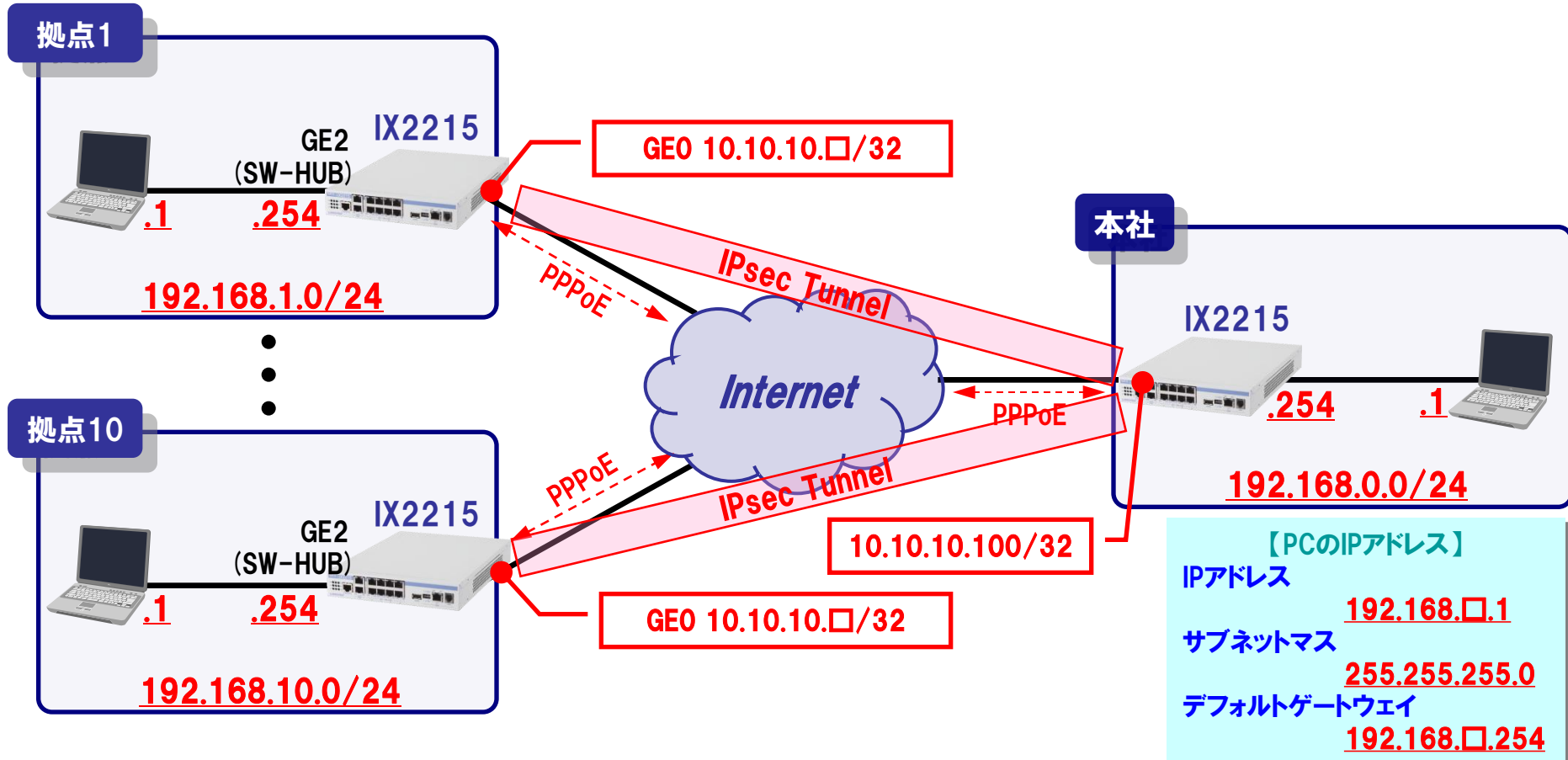
IX3110は最大1,024拠点、
IX3010は最大512拠点、
IX2215/IX2025/IX2105は
最大128拠点との対向が可能。

小規模から中大規模ネットワークのセンタルータまで幅広くご使用いただけます。

高速転送性能

最大スループット（双方向）

IX3110	920Mbps
IX3010	260Mbps
IX2215	1.3 Gbps
IX2025	200Mbps（ヘッダ分含む）
IX2105	440Mbps

目的の構成(インターネットVPN)

■ プロバイダとPPPoE接続、及び、拠点～本社間でのインターネットVPNを構築します。

- 状態表示ランプのPPPランプ/VPNランプが点灯することを確認します。
- 手元のPCから本社のPC「192.168.0.1」宛にpingが通ることを確認します。
- コマンドによりIKE/IPsec SAが確立していることを確認します。

LANインタフェースの設定

GigaEthernet2.0

LANインタフェースの設定（インタフェースコンフィグモード）

```
Router(config)# interface GigaEthernet2.0
Router(config-GigaEthernet2.0)# ip address 192.168.□.254/24
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)#
```

- LANインタフェースの設定
  - IPアドレスの設定
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰

★IPアドレスの第3オクテット目には、**拠点番号(1～10)**を設定してください。

PPPoEインタフェースの設定

GigaEthernet0.1

PPPoEインタフェースの設定

```
Router(config)# ppp profile my-profile
Router(config-ppp-my-profile)# authentication myname test□@test.com
Router(config-ppp-my-profile)# authentication password test□@test.com test□-password
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding my-profile
Router(config-GigaEthernet0.1)# ip address 10.10.10.□/32
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#
```

- PPPプロファイルの設定
  - ppp profile my-profile：ユーザ名／パスワードを設定
  - ppp binding my-profile：PPPoEインタフェースに関連付け
- PPPoEインタフェースの設定
  - IPアドレスの設定

★PPPの認証ID/パスワード、及び、WAN側アドレスの第4オクテット目には**拠点番号(1～10)**を設定してください。

ルーティング設定

スタティックルートの設定

```
Router(config)# ip ufs-cache enable
Router(config)# ip route 10.10.10.100/32 GigaEthernet0.1
Router(config)# ip route default Tunnel0.0
```

- UFSキャッシュの有効化（IPsec転送処理の高速化に必要）
- トンネルの接続先（10.10.10.100）へ到達するためのスタティックルートを設定
  - GigaEthernet0.1：出力先としてWAN回線に接続するPPPoEインタフェースの名前を指定
- トンネル経由で接続先のLANへ到達するためのスタティックルートを設定
  - Tunnel0.0：出力先として本社との接続に使用する仮想トンネルインタフェースの名前を指定
  - トンネルインタフェースをdefaultルートとして指定することで、各拠点からの通信は全て本社経由で行われる。

IPsec/IKEの設定(1)

IKEの設定

```
Router(config)# ike proposal ike-prop encryption aes-256 hash sha lifetime 3600
Router(config)# ike policy ike1 peer 10.10.10.100 key mykey ike-prop
```

・IKE(フェーズ1)の設定

- ike proposal　：暗号/認証アルゴリズム、ライフタイムなどを設定
  - 暗号 AES-256(※)
  - 認証 SHA-1
  - ライフタイム 3,600秒(1時間)

※鍵長の設定はよりセキュリティの強固な
AES(256bit)を選択します。
AES(128/192/256bit)より選択可能。

- ike policy　：ピアアドレス、事前共有鍵などを接続先毎に設定し、使用するIKEプロポーザル関連付け
  - 接続先 10.10.10.100(本社)
  - 事前共有鍵 mykey

注意 暗号/認証アルゴリズム、ライフタイム、事前共有鍵は、IPsecを行う対向装置と同じ値を設定する必要があります。

IPsec/IKEの設定(2)

IPsecの設定

```
Router(config)# ip access-list sec-list permit ip src any dest any
Router(config)# ipsec autokey-proposal ipsec-prop esp-aes-256 esp-sha lifetime time 3600
Router(config)# ipsec autokey-map ipsec1 sec-list peer 10.10.10.100 ipsec-prop
Router(config)# ipsec local-id ipsec1 192.168.□.0/24
Router(config)# ipsec remote-id ipsec1 192.168.0.0/24
```

- IPsec(フェーズ2)の設定
  - ip access-list : アクセスリスト(ACL) IPsec処理を適用するトラフィックを指定。
    - permit 許可/deny 不許可
    - src 送信元アドレス/dest 送信先アドレス(通常any設定で可)
  - ipsec autokey-proposal : カプセル化方式、暗号/認証アルゴリズム、ライフタイムなどを設定
    - カプセル化方式 ESP
    - 暗号 AES-256(※)
    - 認証 SHA-1
    - ライフタイム 3,600秒(1時間)
  - ipsec autokey-map : ピアアドレス、ACL、IPsecプロポーザルなどの指定を接続先毎に設定
  - ipsec local-id : ローカルID
    - 自装置側ID情報をアドレス形式で設定
  - ipsec remote-id : リモートID
    - 相手装置側ID情報をアドレス形式で設定

※鍵長の設定はよりセキュリティの強固な
AES(256bit)を選択します。
AES(128/192/256bit)より選択可能。

ローカルIDとリモートIDの設定は、接続先と必ず対にします。

【注意】 暗号/認証アルゴリズム、ライフタイムは、IPsecを行う対向装置と同じ値を設定する必要があります。

★ローカルIDとして登録するIPアドレスの第3オクテット目には**拠点番号(1～10)**を設定してください。

トンネルインタフェースの設定

トンネルインタフェース(IPsec)の設定

```
Router(config)# interface Tunnel0.0
Router(config-Tunnel0.0)# tunnel mode ipsec
Router(config-Tunnel0.0)# ip unnumbered GigaEthernet2.0
Router(config-Tunnel0.0)# ipsec policy tunnel ipsec1 out
Router(config-Tunnel0.0)# ip tcp adjust-mss auto
Router(config-Tunnel0.0)# no shutdown
Router(config-Tunnel0.0)# exit
Router(config)#
```

- Tunnelインタフェースの設定
  - tunnel mode ipsec　：トンネルモードの選択
  - ip unnumbered　：TunnelインタフェースのIPアドレス設定(本例ではunnumbered設定)
  - ipsec policy　：作成したIPsecポリシーの関連付け

- TCP MSS調整(ip tcp adjust-mss auto)
  - IPsecトンネルを経由するTCPパケットのサイズをTunnelインタフェースのMTU長以下に調整

フィルタ設定

フィルタの設定

```
Router(config)# ip access-list flt-list permit ip src 10.10.10.100/32 dest 10.10.10.□/32
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ip filter flt-list 1 in
Router(config-GigaEthernet0.1)# exit
```

- インターネット側から受信するパケットを、送信元がトンネルの接続先のパケットに限定
- 受信パケットの条件をアクセスリスト(ACL)で指定
  - 送信元 10.10.10.100、宛先 10.10.10.□
- ACLにマッチしなかったパケットは廃棄(暗黙のdeny)
- ip filterコマンドでインタフェースにin方向で適用

★アクセスリストで設定する宛先アドレスの第4オクテット目には**拠点番号(1～10)**を設定してください。

ログ収集の設定と設定保存

ログ収集の設定／設定の保存

```
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory
```

・ログの情報を装置の内部バッファに蓄積

Pingによる疎通の確認

Pingによる疎通の確認（ping 宛先）

IPsecを確立した本社ルータ配下のPCまでの疎通確認を行います。
コマンドプロンプトを起動し、Pingコマンドを実行します。
コマンド：ping 192.168.0.1 [Enter]

```
コマンド プロンプト
C:¥>
C:¥>ping 192.168.0.1

192.168.0.1 に ping を送信しています 32 バイトのデータ:
要求がタイムアウトしました。
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=63
192.168.0.1 からの応答: バイト数 =32 時間 <1ms TTL=63
192.168.0.1 からの応答: バイト数 =32 時間 <1ms TTL=63

192.168.0.1 の ping 統計:
    パケット数: 送信 = 4、受信 = 3、損失 = 1 (25% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 1ms、平均 = 0ms

C:¥>_
```

本例ではPingを4回送信(Sent)して、応答を3パケット受信(Received)している例です。
※初めて疎通確認を行う場合、1つ目のパケットはIPsec確立のトリガーとして使用されるためロスします。

・**応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。**

ログの表示

ログの表示（show logging）

```
Router(config)# show logging
Buffer logging enabled, 131072 bytes, type cyclic
  18 messages (1-18), 1389 bytes logged, 0 messages dropped

Log Buffer (1-13):
2013/10/18 15:19:19   GW.038: User anonymous@ has logged on
2013/10/18 15:19:27  ETH.031: Link status up for port 0, 100M b/s, GigaEthernet0
2013/10/18 15:19:27   IP.021: Interface GigaEthernet0.1, link up
2013/10/18 15:19:27  ETH.031: Link status up for port 1, 100M b/s, GigaEthernet2
2013/10/18 15:19:27   IP.021: Interface GigaEthernet2.0, link up
2013/10/18 15:19:27   IP.021: Interface GigaEthernet2.0, line protocol up
2013/10/18 15:19:27   IP.021: Interface GigaEthernet2.0, up
2013/10/18 15:19:58 PPOE.029: Session start, AccessCT address 00:26:99:db:b4:58, SessionID 1218,
GigaEthernet0.1
2013/10/18 15:19:58  PPP.004: LCP OPENING: state is open, opening upper-link, on GigaEthernet0.1
2013/10/18 15:19:58  PPP.001: NCP OPENING: IPCP state is open, opening upper-link, on GigaEthernet0.1
2013/10/18 15:19:58   IP.021: Interface GigaEthernet0.1, line protocol up
2013/10/18 15:19:58   IP.021: Interface GigaEthernet0.1, up
2013/10/18 15:19:59   IP.021: Interface Tunnel0.0, link up
2013/10/18 15:19:59   IP.021: Interface Tunnel0.0, link down
2013/10/18 15:19:59   IP.021: Interface Tunnel0.0, link up
2013/10/18 14:19:59   IP.021: Interface Tunnel0.0, line protocol up
2013/10/18 15:19:59   IP.021: Interface Tunnel0.0, up
2013/10/18 15:22:19   GW.079: System woke up by reload, caused by power-on. System started at Oct 18-
Fri-2013 15:19:11 JST
```

- 電源ON後のログ情報を表示します。
- ログの削除には「clear logging」コマンドを使用します。
- インタフェースのlink-up/link-down発生日時などを確認することができます。
- IPsec/ISAKMP SAが正常に確立しない場合、その理由を確認することができます。

ルーティングテーブルの表示

ルーティングテーブルの表示（show ip route）

```
Router(config)# show ip route
IP Routing Table - 5 entries, 2 hidden, 2041 frees
Entries: 3 Connected, 2 Static, 0 RIP, 0 OSPF, 0 BGP
Codes: C - Connected, S - Static, R - RIP, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, B - BGP
       * - Candidate default, s - Summary
Timers: Age
S*    0.0.0.0/0 [1/1] is directly connected, Tunnel0.0, 0:05:04
      10.0.0.0/8 is subnetted, 2 subnets
C       10.10.10.1/32 [0/1] is directly connected, GigaEthernet0.1, 0:15:45
S       10.10.10.100/32 [1/1] is directly connected, GigaEthernet0.1, 0:11:06
C     192.168.1.0/24 [0/1] is directly connected, GigaEthernet2.0, 0:27:39
      200.200.200.0/24 is subnetted, 1 subnets
C       200.200.200.1/32 [0/1] is directly connected, GigaEthernet0.1, 0:15:45
```

- 「show ip route」コマンドにより、IPの経路情報テーブルを表示させることが可能です。
- 目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りが無いかを確認する場合に利用します。

PPPoE接続状態の確認

PPPoE接続状態の確認（show ip address）

```
Router(config)# show ip address GigaEthernet0.1
Interface GigaEthernet0.1 is up, line protocol is up
  Internet address is 10.10.10.1/32
  Broadcast address is 255.255.255.255
  Peer address is 200.200.200.1
  Address determined by config
```

- 「show ip address」コマンドにより、PPPoE接続状態の確認が可能です。
- show ip address <I/F NAME>
  - **up**：PPPoEセッション確立
  - **dormant**：PPPoEセッション未確立（ポートup）
    - 網側とPPPoE通信が正常にできていない。
    - PPPのユーザ名／パスワードに誤りがある。
  - **down**：PPPoEセッション未確立（ポートdown）

PPPoEが接続すると装置前面のPPPランプが点灯します。

点灯：接続
消灯：未接続
点滅：ネゴシエーション中

PPPランプが点滅のまま変わらない場合は、認証が失敗している可能性があります。設定したユーザIDとパスワード設定に誤りが無いか見直しをして下さい。

IPsec/IKEの状態表示(1)

ISAKMP SAの表示

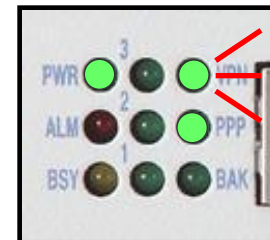
```
Router(config)# show ike sa
ISAKMP SA - 1 configured, 1 created
Local address is 10.10.10.1, port is 500
Remote address is 10.10.10.100, port is 500
  IKE policy name is ike1
  Direction is initiator
  Initiator's cookie is 0x06bf457d1fed7730
  Responder's cookie is 0x6188dcff400bfd7b
  Exchange type is main mode
  State is established
  Authentication method is pre-shared
  Encryption algorithm is aes-256
  Hash algorithm is sha1
  DH group is modp768, lifetime is 3545 seconds
  #ph1 success: 1, #ph1 failure: 0
  #ph1 hash err: 0, #ph1 timeout: 0, #ph1 resend: 0
  #ph2 success: 1, #ph2 failure: 0
  #ph2 hash err: 0, #ph2 timeout: 0, #ph2 resend: 0
```

- 状態(State)が「established」と表示されていることを確認します。
- ISAKMP SAが出来ていれば、SAの情報(cookie、ライフタイムなど)が表示されます

IPsec/IKEの状態表示(2)

IPsec SAの表示

```
Router(config)# show ipsec sa
IPsec SA - 1 configured, 2 created
Interface is Tunnel0.0
  Key policy map name is ipsec1
    Tunnel mode, 4-over-4, autokey-map
    Local address is 10.10.10.1
    Remote address is 10.10.10.100
    Outgoing interface is GigaEthernet0.1
    Interface MTU is 1390, path MTU is 1454
    Inbound:
      ESP, SPI is 0x54fddfbb(1425924027)
        Transform is ESP-AES-256-HMAC-SHA-96
        Remaining lifetime is 3542 seconds
      Replay detection support is on
    Outbound:
      ESP, SPI is 0x8854402f(2287222831)
        Transform is ESP-AES-256-HMAC-SHA-96
        Remaining lifetime is 3542 seconds
      Replay detection support is on
    Perfect forward secrecy is off
```

IPsec SAが確立すると装置前面の
VPNランプが点灯します。

点灯:接続
消灯:未接続

VPNランプが点灯しない場合、ISAKMP SAや
IPsec SAの表示が異なる場合は、
前のページで設定した内容に誤りが無いか
見直しをして下さい。

- IPsec SAが出来ていれば、Inbound/OutboundそれぞれのSAの情報(SPI値、ライフタイムなど)が表示されます
- TunnelインタフェースのMTU長は、出力インタフェースのMTU長から自動計算します

IPsec/IKEの状態表示(3)

SAの簡易表示

```
Router(config)# show ike sa brief
ISAKMP SA - 2 configured, 2 created
Policy                         Initiator          Responder          Life(secs)
ike1                           0x06bf457d1fed7730 0x6188dcff400bfd7b   3257
ike2                           0xe84885d607c84fcf 0xb3da55732d2f5f81   3481


Router(config)# show ipsec sa brief
IPsec SA - 2 configured, 4 created
Policy map                       Dir   Type   SPI           Life(secs/bytes)
ipsec1                           IN    ESP    0x54fddfbb      3255/-
ipsec1                           OUT   ESP    0x8854402f      3255/-
ipsec2                           IN    ESP    0xd83e9ac9      3573/-
ipsec2                           OUT   ESP    0x9df25dee      3573/-
```

・briefオプションを付加することにより、簡易表示モードに切り替わります
・センタ側装置で、各接続先とのSA確立状態を一覧表示したいときに便利

目次

演習3に登場する主な用語

★**EtherIP** (Ethernet over IP)
イーサアイピー

イーサネットフレームをIPでカプセル化（トンネリング）することにより、非IPのトラフィックをIPネットワーク上で転送できるようにするプロトコル。
物理的に離れた拠点間を、IPネットワークを介して同一LANとして接続するL2-VPNの構築にも使われる。

★**L2-VPN** (Layer2 Virtual Private Network)
レイヤー2 ブイピーエヌ

イーサネットなどのレイヤ2フレームを配送することのできるVPN（仮想的な閉域網）のこと。
EtherIPやL2TPなどがある。
一方、インターネットVPNの構築で一般的に使われるIPsec（トンネルモード）はレイヤ3プロトコルであるIPのみ扱うことが可能なため、L3-VPNに分類される。

★**IRB** (Integrated Routing and Bridging)
アイアールビー

異なるブリッジのグループ間、及びブリッジではないインタフェース間の通信（ルーティング）を実現する機能。

★**BVI** (Bridging Virtual Interface)
ビーブイアイ インタフェース

ブリッジモードで動作するインタフェースにおいて、IPトラフィックの送受信を行うためのインタフェース。

★**IPsecトランスポートモード**

EtherIPとIPsecを併用する場合、EtherIPのカプセル化処理によりトンネル用IPヘッダが付与されるため、IPsecはデータ部のみ暗号化するトランスポートモードを使用することができる。
（IPsecトンネルモードを使用すると、トンネル用のIPヘッダが二重に付与されるためオーバヘッドが増える。）

EtherIP機能（Ethernet over IP）

- 離れた拠点間をインターネットを介してブリッジ接続することが可能です。
- インターネットVPNやIP-VPNサービスに非IP端末を収容できるようになります。
- IPパケットの転送が可能であれば、回線種別を問わず利用可能です。

EtherフレームをIPヘッダでカプセル化。
IPsecと組み合わせて使用することで
セキュリティも安心

本社

非IP端末

EtherIP（IPsec）トンネル

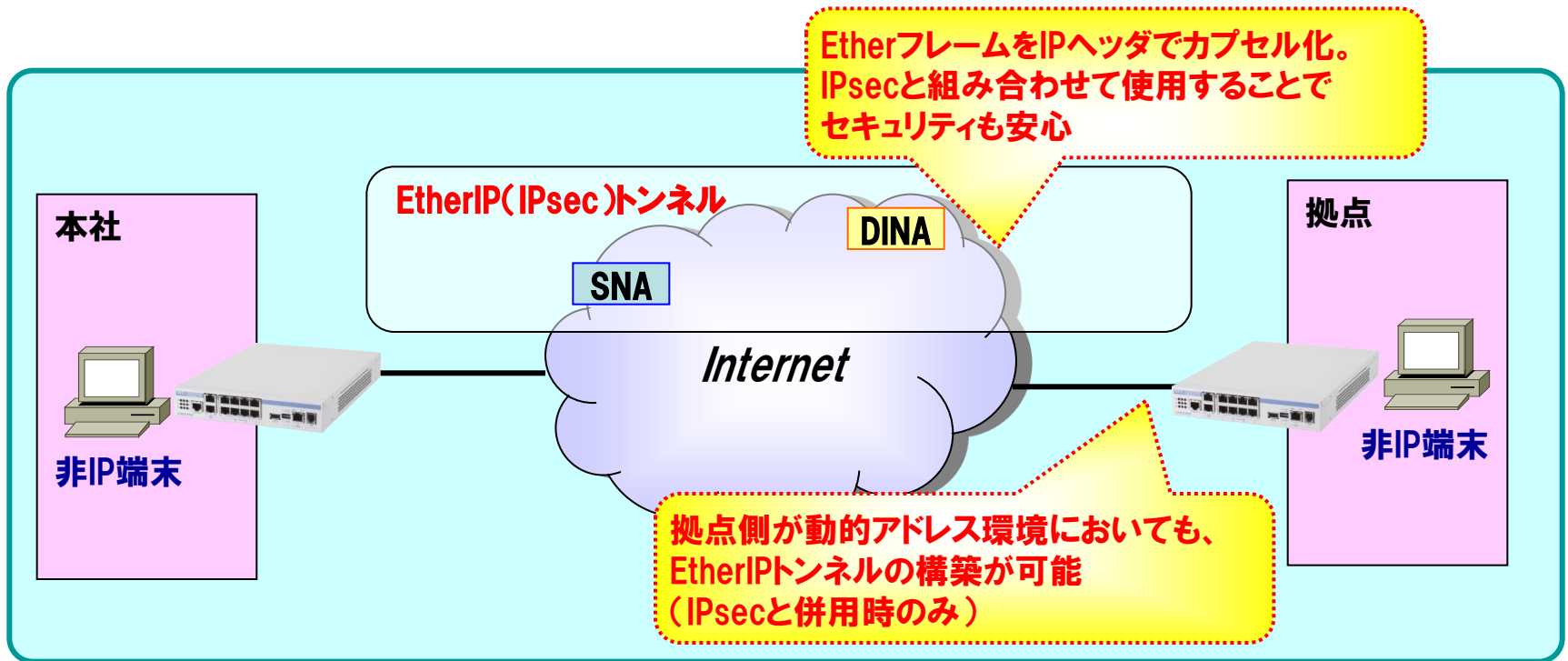
DINA

SNA

Internet

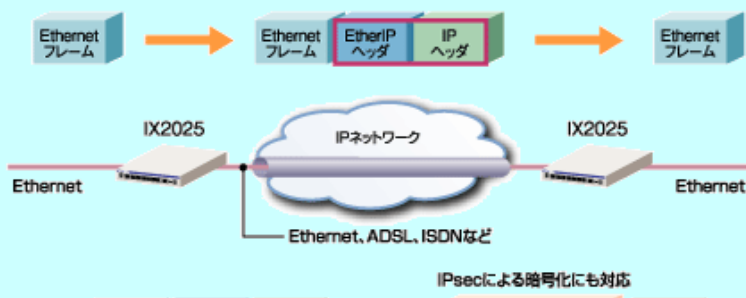
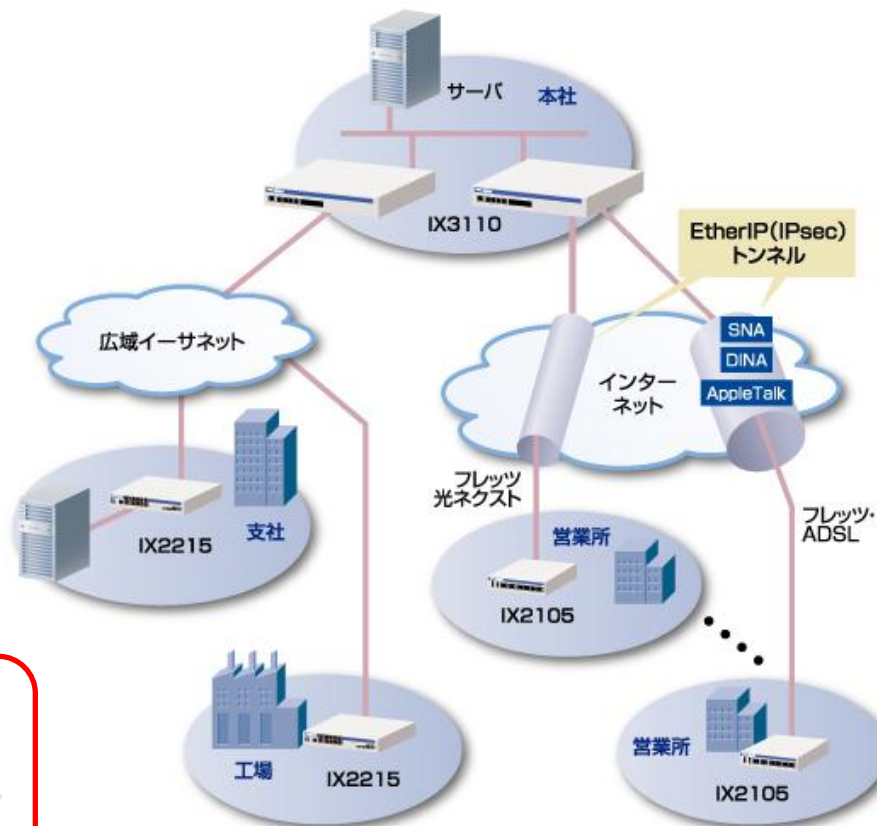
拠点

非IP端末

拠点側が動的アドレス環境においても、
EtherIPトンネルの構築が可能
（IPsecと併用時のみ）

Ver.8.9以降、Ether over GREにも対応

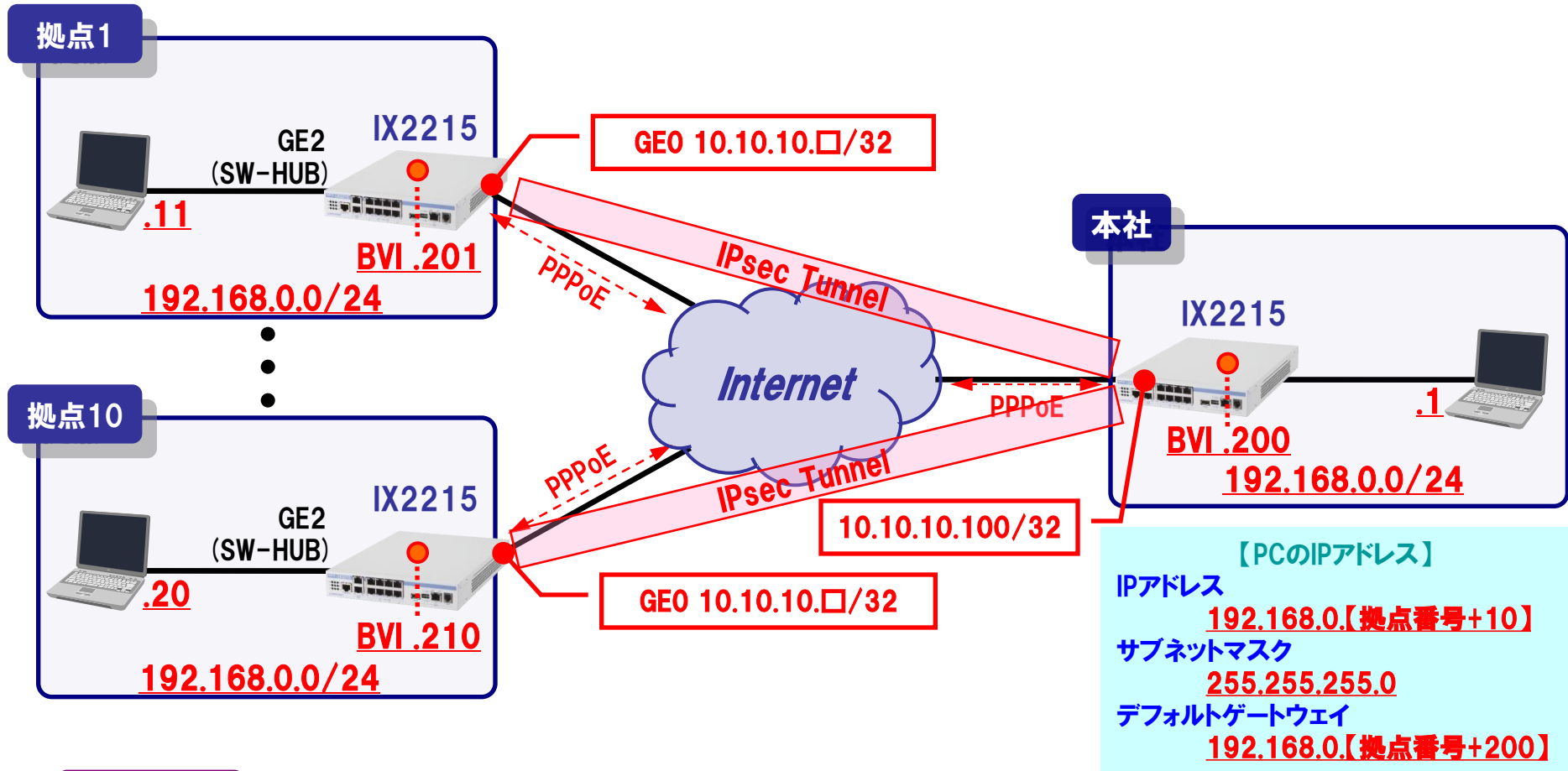
Empowered by Innovation

EtherIPによるL2-VPNネットワーク

- EtherIP（Etherフレームを IPヘッダでカプセル化する技術）を使用して、インターネットのような**「IPネットワーク」上で、L2-VPNを実現**することが可能です。
また、**IPsecとの併用も可能**なのでセキュリティを保護できます。

重要な支社や工場は信頼性の高い広域イーサネットを使用。営業所などはインターネット回線を使用してIPsecを併用することにより、安価で安全なネットワークを構築可能です！

IXルータのEtherIP特長

高速転送性能	IX3110で最大2.3Gbps、IX3010（2GE-Tカード使用時）で最大830Mbps、IX2215で最大2.0Gbps、IX2025で最大200Mbps、IX2105で最大1Gbpsの転送性能を実現。また、IPsec併用時でも、高速転送が可能です。
セキュリティ	IPsecとの併用が可能で、インターネット上でも安心してブリッジ網の構築が可能です。また、MACフィルタリングにより、ブリッジしたくないフレームを遮断することも可能です。
ブリッジとの併用	従来のブリッジ機能と併用して利用可能です。 ブリッジに属するLANインタフェースとEtherIPトンネルをグループ分けすることで、VLANの形成が可能です。
低コスト	トンネルの一方が動的IPの構成でもEtherIPトンネルの確立が可能です。 （IPsec/IKEとの併用が必須）
対地数	IX3110で最大200対地、IX3010で最大50対地までの収容が可能です。 （IX2215/IX2025/IX2105で10対地）。
QoS	EtherIPトンネルでカプセル化したフレームに対しても、カプセル化前のフレームの情報を元に優先制御することが可能です。

目的の構成 (EtherIP w/IPsec)

■ プロバイダとPPPoE接続、及び、拠点～本社間でのL2-VPN (EtherIP) を構築します。

拠点1

IX2215

GE2
(SW-HUB)

.11

BVI .201

192.168.0.0/24

GE0 10.10.10.□/32

PPPoE

IPsec Tunnel

Internet

本社

IX2215

.1

BVI .200

192.168.0.0/24

PPPoE

10.10.10.100/32

拠点10

IX2215

GE2
(SW-HUB)

.20

BVI .210

192.168.0.0/24

PPPoE

IPsec Tunnel

GE0 10.10.10.□/32

【PCのIPアドレス】

IPアドレス
192.168.0.【拠点番号+10】

サブネットマスク
255.255.255.0

デフォルトゲートウェイ
192.168.0.【拠点番号+200】

- ☑ 状態表示ランプのPPPランプ/VPNランプが点灯することを確認します。
- ☑ 手元のPCから本社のPC「192.168.0.1」宛にpingが通ることを確認します。
- ☑ コマンドによりIKE/IPsec SAとEtherIP (ブリッジ) の状態を確認します。

LAN／BVIインタフェースの設定

GigaEthernet2.0

LANインタフェース/BVIインタフェースの設定（インタフェースコンフィグモード）

```
Router(config)# bridge irb enable
Router(config)# interface GigaEthernet2.0
Router(config-GigaEthernet2.0)# bridge-group 1
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)# interface BVI0
Router(config-BVI0)# bridge-group 1
Router(config-BVI0)# ip address 192.168.0.□/24
Router(config-BVI0)# no shutdown                ↑ 拠点番号＋200 の値を入力
Router(config-BVI0)# exit
Router(config)#
```

- ブリッジ機能の有効化(bridge irb enable)
- LANインタフェースの設定
  - ブリッジグループの設定(同じグループに属するインタフェースは同一LANとなる)
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰
- BVIインタフェースの設定(ブリッジ動作時の保守用インタフェース)
  - ブリッジグループの設定
  - IPアドレス設定
  - no shutdown

BVIインタフェースのIPアドレス

拠点	IPアドレス
拠点 1	192.168.0.201/24
拠点 2	192.168.0.202/24
拠点 3	192.168.0.203/24
拠点 4	192.168.0.204/24
拠点 5	192.168.0.205/24
拠点 6	192.168.0.206/24
拠点 7	192.168.0.207/24
拠点 8	192.168.0.208/24
拠点 9	192.168.0.209/24
拠点10	192.168.0.210/24

★BVIインタフェースに設定するIPアドレスの第4オクテット目には「拠点番号（1～10）＋200」を設定してください。

PPPoEインタフェースの設定

PPPoEインタフェースの設定

```
Router(config)# ppp profile my-profile
Router(config-ppp-my-profile)# authentication myname test□@test.com
Router(config-ppp-my-profile)# authentication password test□@test.com test□-password
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding my-profile
Router(config-GigaEthernet0.1)# ip address 10.10.10.□/32
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#
```

- **PPPプロファイルの設定**
  - ppp profile my-profile：ユーザ名／パスワードを設定
  - ppp binding my-profile：PPPoEインタフェースに関連付け
- **PPPoEインタフェースの設定**
  - IPアドレスの設定

★PPPの認証ID/パスワード、及び、WAN側アドレスの第4オクテット目には**拠点番号(1～10)**を設定してください。

ルーティング設定

スタティックルートの設定

```
Router(config)# ip ufs-cache enable
Router(config)# ip route 10.10.10.100/32 GigaEthernet0.1
```

・UFSキャッシュの有効化(IPsec転送処理高速化に必要)

・トンネルの接続先(10.10.10.100)へ到達するためのスタティックルートを設定

 – GigaEthernet0.1：出力先としてWAN回線に接続するPPPoEインタフェースの名前を指定

IPsec/IKEの設定（1）

IKEの設定

```
Router(config)# ike proposal ike-prop encryption aes-256 hash sha lifetime 3600
Router(config)# ike policy ike1 peer 10.10.10.100 key mykey ike-prop
```

・IKEの設定
- ike proposal　：暗号/認証アルゴリズム、ライフタイムなどを設定
  - 暗号 AES-256（※）
  - 認証 SHA-1
  - ライフタイム 3,600秒（1時間）

※鍵長の設定はよりセキュリティの強固な
AES（256bit）を選択します。
AES（128/192/256bit）より選択可能。

- ike policy　：ピアアドレス、事前共有鍵などを接続先毎に設定し、使用するIKEプロポーザル関連付け
  - 接続先 10.10.10.100（本社）
  - 事前共有鍵 mykey

|注意| 暗号/認証アルゴリズム、ライフタイム、事前共有鍵は、IPsecを行う対向装置と同じ値を設定する必要があります。

IPsec/IKEの設定(2)

IPsecの設定

```
Router(config)# ip access-list sec-list permit ip src any dest any
Router(config)# ipsec autokey-proposal ipsec-prop esp-aes-256 esp-sha lifetime time 3600
Router(config)# ipsec autokey-map ipsec1 sec-list peer 10.10.10.100 ipsec-prop
Router(config)# ipsec local-id ipsec1 10.10.10.□
Router(config)# ipsec remote-id ipsec1 10.10.10.100
```

- IPsecの設定
  - アクセスリスト(ACL) ：IPsec処理を適用するトラフィックを指定。通常Any設定で可。
  - ipsec autokey-proposal ：カプセル化方式、暗号/認証アルゴリズム、ライフタイムなどを設定
    - カプセル化方式 ESP
    - 暗号 AES-256(※)
    - 認証 SHA-1
    - ライフタイム 3,600秒(1時間)
  - ipsec autokey-map ：ピアアドレス、ACL、IPsecプロポーザルなどの指定を接続先毎に設定
  - ipsec local-id ：ローカルID
    - 自装置側ID情報をアドレス形式で設定
  - ipsec remote-id ：リモートID
    - 相手装置側ID情報をアドレス形式で設定

※鍵長の設定はよりセキュリティの強固な
AES(256bit)を選択します。
AES(128/192/256bit)より選択可能。

ローカルIDとリモートIDの設定は、接続先と必ず対にします

|注意| 暗号/認証アルゴリズム、ライフタイム、事前共有鍵は、IPsecを行う対向装置と同じ値を設定する必要があります。

★ローカルIDとして登録するIPアドレスの第4オクテット目には拠点番号(1～10)を設定してください。

トンネルインタフェースの設定

トンネルインタフェース(Etherip w/IPsec)の設定

```
Router(config)# interface Tunnel0.0
Router(config-Tunnel0.0)# tunnel mode ether-ip ipsec
Router(config-Tunnel0.0)# bridge-group 1
Router(config-Tunnel0.0)# ipsec policy transport ipsec1 with-id-payload
Router(config-Tunnel0.0)# bridge ip tcp adjust-mss 1300
Router(config-Tunnel0.0)# no shutdown
Router(config-Tunnel0.0)# exit
Router(config)#
```

- Tunnelインタフェースの設定
  - tunnel mode etherip ipsec:トンネルモードの選択
  - ipsec policy　　　　　:作成したIPsecポリシーの関連付け(トランスポートモード)
  - bridge-group 1　　　　:LANインタフェースと同じブリッジグループに設定

- TCP MSS調整(bridge ip tcp adjust-mss 1300)
  - IPsecトンネルを経由するTCPパケットのサイズをTunnelインタフェースのMTU長以下に調整
  - ip tcp adjust-mssコマンドと異なり、MSS値は手動設定にのみ対応。

フィルタ設定

フィルタの設定

```
Router(config)# ip access-list flt-list permit ip src 10.10.10.100/32 dest 10.10.10.□/32
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ip filter flt-list 1 in
Router(config-GigaEthernet0.1)# exit
```

- インターネット側から受信するパケットを、送信元がトンネルの接続先のパケットに限定
- 受信パケットの条件をアクセスリスト(ACL)で指定
  - 送信元 10.10.10.100、宛先 10.10.10.□
- ACLにマッチしなかったパケットは廃棄(暗黙のdeny)
- ip filterコマンドでインタフェースにin方向で適用

★アクセスリストで設定する宛先アドレスの第4オクテット目には**拠点番号(1～10)**を設定してください。

ログ収集の設定と設定保存

ログ収集の設定／設定の保存

```
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory
```

・ログの情報を装置の内部バッファに蓄積

Pingによる疎通の確認

Pingによる疎通の確認（ping 宛先）

EtherIP w/IPsecを確立した本社ルータ配下のPCまでの疎通確認を行います。
コマンドプロンプトを起動し、Pingコマンドを実行します。
コマンド ： ping 192.168.0.1 [Enter]

```
コマンド プロンプト
C:¥>
C:¥>ping 192.168.0.1

192.168.0.1 に ping を送信しています 32 バイトのデータ:
要求がタイムアウトしました。
192.168.0.1 からの応答: バイト数 =32 時間 =1ms TTL=63
192.168.0.1 からの応答: バイト数 =32 時間 <1ms TTL=63
192.168.0.1 からの応答: バイト数 =32 時間 <1ms TTL=63

192.168.0.1 の ping 統計:
    パケット数: 送信 = 4、受信 = 3、損失 = 1 (25% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 1ms、平均 = 0ms

C:¥>_
```

本例ではPingを4回送信（Sent）して、応答を3パケット受信（Received）している例です。
※初めて疎通確認を行う場合、1つ目のパケットはIPsec確立のトリガーとして使用されるためロスします。

・応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。

Empowered by Innovation

IPsec/IKEの状態表示(1)

ISAKMP SAの表示

```
Router(config)# show ike sa
ISAKMP SA - 1 configured, 1 created
Local address is 10.10.10.1, port is 500
Remote address is 10.10.10.100, port is 500
  IKE policy name is ike1
  Direction is initiator
  Initiator's cookie is 0x4e70cb5efa7df1ad
  Responder's cookie is 0xc9673e549814db8d
  Exchange type is main mode
  State is established
  Authentication method is pre-shared
  Encryption algorithm is aes-256
  Hash algorithm is sha1
  DH group is modp768, lifetime is 3519 seconds
  #ph1 success: 1, #ph1 failure: 0
  #ph1 hash err: 0, #ph1 timeout: 0, #ph1 resend: 0
  #ph2 success: 1, #ph2 failure: 0
  #ph2 hash err: 0, #ph2 timeout: 0, #ph2 resend: 0
```

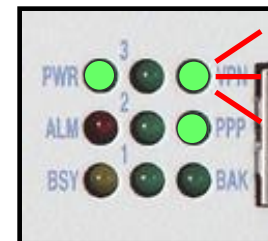
・状態(State)が「established」と表示されていることを確認します。

・ISAKMP SAが出来ていれば、SAの情報(cookie、ライフタイムなど)が表示されます。

IPsec/IKEの状態表示(2)

IPsec SAの表示

```
Router(config)# show ipsec sa
IPsec SA - 1 configured, 2 created
Interface is Tunnel0.0
  Key policy map name is ipsec1
    Transport mode, autokey-map
    Local address is 10.10.10.1
    Remote address is 10.10.10.100
    Outgoing interface is GigaEthernet0.1
    Interface MTU is 1410, path MTU is 1454
    Inbound:
      ESP, SPI is 0xa7306f83(2804969347)
        Transform is ESP-AES-256-HMAC-SHA-96
        Remaining lifetime is 3515 seconds
      Replay detection support is on
    Outbound:
      ESP, SPI is 0xb3158428(3004531752)
        Transform is ESP-AES-256-HMAC-SHA-96
        Remaining lifetime is 3515 seconds
      Replay detection support is on
    Perfect forward secrecy is off
```

IPsec SAが確立すると装置前面の
VPNランプが点灯します。

点灯:接続
消灯:未接続

VPNランプが点灯しない場合、ISAKMP SAや
IPsec SAの表示が異なる場合は、
前のページで設定した内容に誤りが無いか
見直しをして下さい。

- IPsec SAが出来ていれば、Inbound/OutboundそれぞれのSAの情報(SPI値、ライフタイムなど)が表示されます
- TunnelインタフェースのMTU長は、出力インタフェースのMTU長から自動計算します

ブリッジの動作状態の表示

ブリッジ状態の表示

```
Router(config)# show bridge
IRB Group 1 Forwarding Cache - 3 entries, 4093 frees, 338 flybys, 0 overflows
Codes: P - permanent, B - BVI
  BG       Address        Interface             Timeout   RX count   TX count
   1 00:60:b9:4e:b5:4d Tunnel0.0                    261         13         13
B  1 00:60:b9:4e:fd:9a BVI0                           -          1          0
   1 fc:61:98:0c:29:36 GigaEthernet2.0              261        353         22

IRB Group 1:
  Interface             Status       Address            RX count   TX count
  BVI0                  forward 00:60:b9:4e:fd:9a          11        340
  GigaEthernet2.0       forward 00:60:b9:4e:fd:9a         353         24
  Tunnel0.0             forward --:--:--:--:--:--          13         46
```

- ブリッジに設定したインタフェースの状態が全て「forward」になっていることを確認
- 状態が「forward」になっているにも関わらず、通信不可の場合には、パケット送受信の統計（RX/TX count）を見てトラフィックの状態を確認

目次

参考演習に登場する用語

★RA (Router Advertisement)
アールエー

IPv6機能を有したルータが、プレフィックスなどの情報を広告する際に出力するメッセージ。
メッセージには、フラグやMTU長、ルータライフタイムなどが含まれる。

★ND (Neighbor Discovery)
ネイバーディスカバリー

同一セグメント上の隣接装置の情報を探索する機能。
IPv4のARP相当の機能などが含まれる。

★ネットワークID

IPv4でのネットワークアドレス相当。
IPv6アドレスの前半64bit (4オクテット) で構成。

★インターフェースID

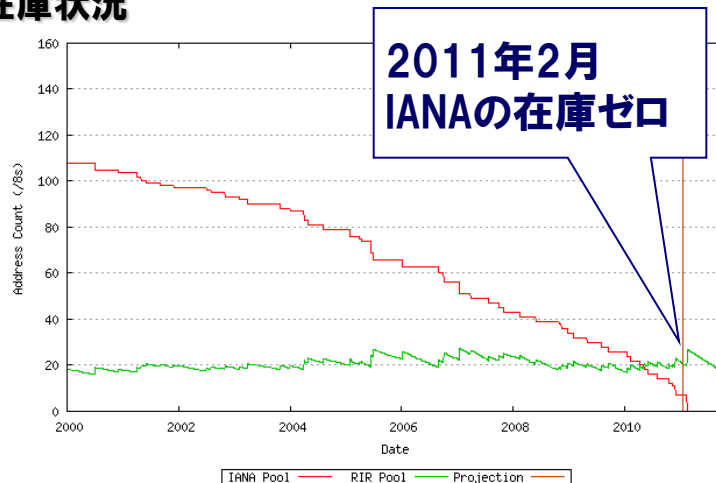
IPv4でのホストアドレス相当。
IPv6アドレスの後半64bit (4オクテット) で構成。

★VRRPv3 (Virtual Router Redundancy Protocol version3)

VRRPのIPv6対応版。
LAN側でIPv6を使用している場合のゲートウェイ冗長化時に使用。

IPv4アドレスの現状

IPv4アドレスの枯渇とIPv6対応

- 2011年2月のIPv4アドレスのセンタ在庫(IANA在庫)枯渇に続き、2011年4月には、日本のIPv4アドレスを管理するJPNICの在庫が枯渇しました。
- 企業ネットワークのIPv6対応が喫緊の課題となっています。

2011年4月15日
JPNICの在庫も枯渇

今後はプロバイダの在庫のみでのアドレス運用になり、数年内での枯渇が予測されています。
プロバイダ接続部分をIPv6対応に切り替えていく必要があります。

IPv6アドレス

IPv6アドレス特徴

- IPv6アドレスは、16進 16Bit (4桁) 8オクテットの128ビットで構成。
  区切り文字は“ : ”(コロン)を使用
- 先頭4オクテットをネットワークID、後半4オクテットをインターフェースIDで構成。

▼ IPv6アドレスの表記

・128bit を 16bit 毎に 8分割後、各フィールドを 16進数表記にして “ : ”(コロン)で区切る。

00100000000000010000110110111000000000000000000000000000000000000000001000000110001010011111111111111110000111100100100000101110

↓

2001:0db8:0000:0000:0206:29ff:fe1e:482e

・先行する 0 は省略可能。但し、各フィールドには少なくとも 1つの数値を含むこと。

2001:0db8:0000:0000:0206:29ff:fe1e:482e

↓

2001:db8:0:0:206:29ff:fe1e:482e

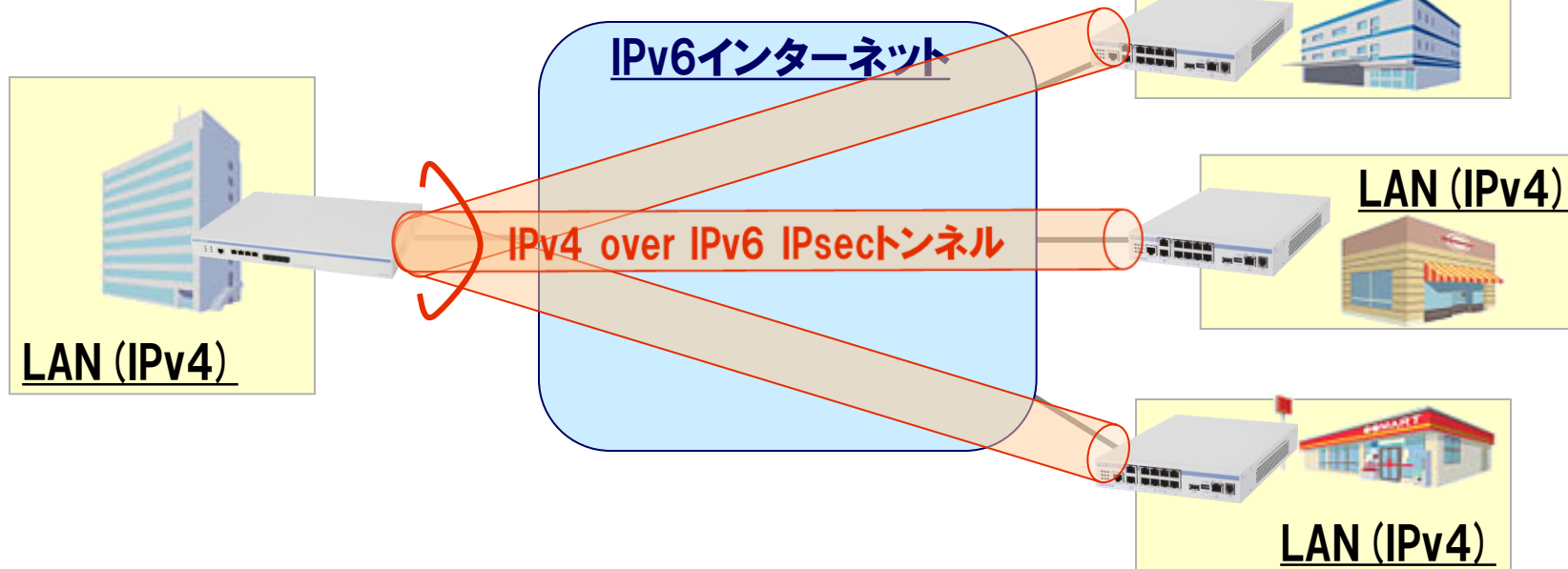
・16bit の 0 または、16bit の 0 が複数連続するフィールドを1箇所のみ” :: ” を用いて省略可能。

2001:db8:0:0:206:29ff:fe1e:482e

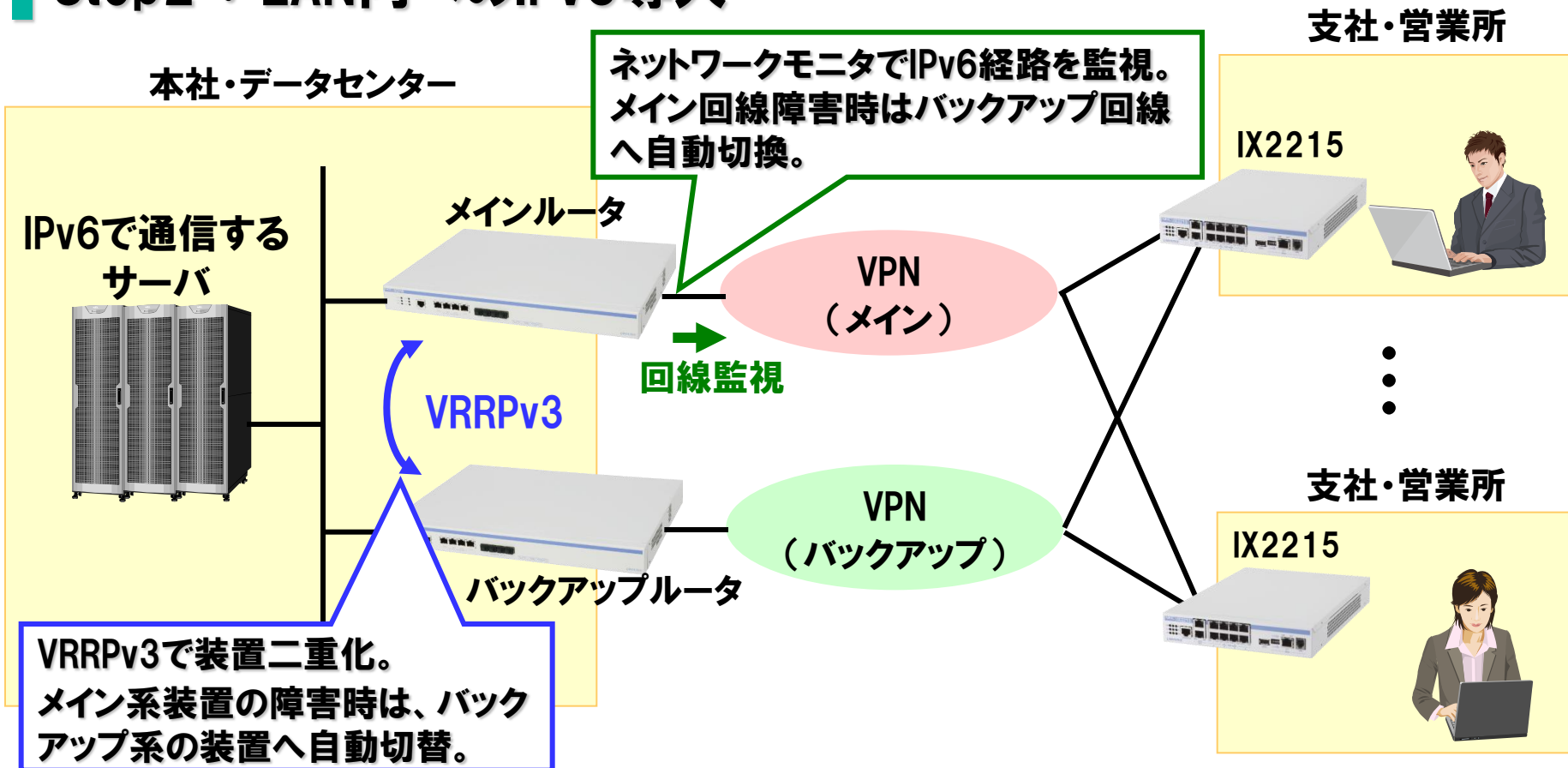
↓

2001:db8::206:29ff:fe1e:482e

IXルータを使用したIPv6への移行シナリオ（1）

Step1 ：WAN回線のIPv6化

IPv4が実際に枯渇しても、今のうちにIPv6に切り替えておけば安心。
また、フレッツ光ネクストご利用中であれば、**追加コストはかかりません**。

IXルータを使用したIPv6への移行シナリオ（2）

Step2 ： LAN内へのIPv6導入

VRRPv3やネットワークモニタ機能を使用して、
IPv4と同等の高信頼ネットワークを提供可能！！

目的の構成（IPv6）

■ WAN、及び、LANをIPv6アドレスを使用して構築します。

拠点1

IX2215

GE2
(SW-HUB)

::cafe

自動設定

2001:db8:1::/64

GE0 2001:db8::11/64

本社

IX2215

::cafe

::ace

2001:db8:100::/64

IPv6-NW

2001:db8::/64

2001:db8::beef/64

拠点10

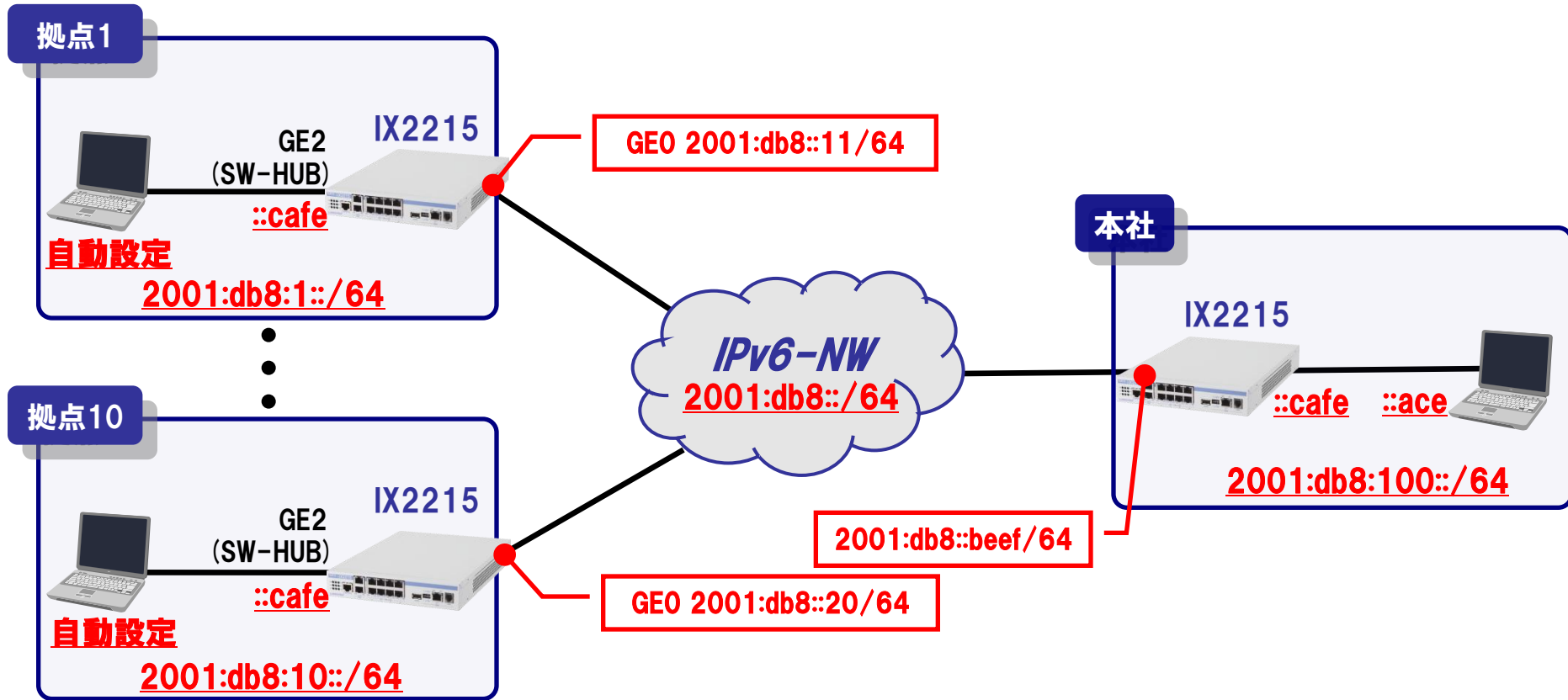
IX2215

GE2
(SW-HUB)

::cafe

自動設定

2001:db8:10::/64

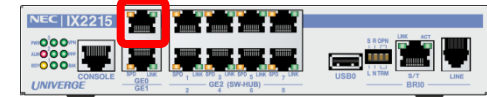
GE0 2001:db8::20/64

- コマンドプロンプトから、PCにアドレスが自動設定されていることを確認します。
- 手元のPCから本社のPC「2001:db8:100::ace」宛にpingが通ることを確認します。

WANインタフェースの設定

GigaEthernet0.0

WANインタフェース（インタフェースコンフィグモード）

```
Router(config)# interface GigaEthernet0.0
Router(config-GigaEthernet0.0)# ipv6 enable
Router(config-GigaEthernet0.0)# ipv6 address 2001:db8::□/64
Router(config-GigaEthernet0.0)# no shutdown
Router(config-GigaEthernet0.0)# exit
Router(config)#
```

↑ 拠点番号＋10を入力

- WANインタフェースの設定
  - IPv6機能の有効化
  - アドレスの設定
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰

GE0のIPv6アドレス

拠点	アドレス
拠点 1	2001:db8::11/64
拠点 2	2001:db8::12/64
拠点 3	2001:db8::13/64
拠点 4	2001:db8::14/64
拠点 5	2001:db8::15/64
拠点 6	2001:db8::16/64
拠点 7	2001:db8::17/64
拠点 8	2001:db8::18/64
拠点 9	2001:db8::19/64
拠点10	2001:db8::20/64

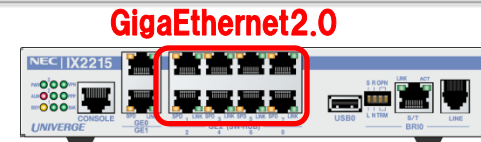
★インタフェースに設定するIPアドレス第8オクテット目には「拠点番号（1～10）＋10 」を設定してください。

LANインタフェースの設定

GigaEthernet2.0

LANインタフェース（インタフェースコンフィグモード）

```
Router(config)# interface GigaEthernet2.0
Router(config-GigaEthernet2.0)# ipv6 enable
Router(config-GigaEthernet2.0)# ipv6 address 2001:db8:□::cafe/64
Router(config-GigaEthernet2.0)# ipv6 nd ra enable
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)#
```

↑ 拠点番号を入力

- LANインタフェースの設定
  - IPv6機能の有効化
  - アドレスの設定
  - ルータ通知メッセージ送信の設定
  - no shutdownコマンドでインタフェース有効化
  - exit で上位モードに復帰

★インタフェースに設定するIPアドレスの第3オクテット目には「拠点番号（1～10）」を設定してください。

ルーティング設定

スタティックルートの設定

```
Router(config)# ipv6 route 2001:db8:100::/64 2001:db8::beef
```

- 接続先(2001:db8:100::/64)へ到達するためのスタティックルートを設定
  - 出力先としてWAN回線のピアアドレスを指定

IPv6アドレスの確認

端末のIPアドレスの確認

端末のアドレス確認を行います。
コマンドプロンプトを起動し、ipconfigコマンドを実行します。
コマンド ： ipconfig ［Enter］

Pingによる疎通の確認

Pingによる疎通の確認（ping 宛先）

本社側の端末までの疎通確認を行います。
コマンドプロンプトを起動し、Pingコマンドを実行します。
コマンド ： ping 2001:db8:100::ace [Enter]

本例ではPingを4回送信して、応答を4パケット受信している例です。パケットロスが0であることを確認します。

・応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。

現在の設定の表示

現在の設定の表示（show running-config）

```
Router(config)# show running-config
Current configuration : 1097 bytes
! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 8.10.11, RELEASE
SOFTWARE
! Compiled Aug 02-Fri-2013 13:34:44 JST #2
! Current time Oct 18-Fri-2013 15:32:12 JST
!
timezone +09 00
!
ipv6 route 2001:db8:100::/64 2001:db8::beef
!
interface GigaEthernet0.0
  no ip address
  ipv6 enable                  ↓ 拠点番号＋10を入力
  ipv6 address 2001:db8::11/64
  no shutdown
!
interface GigaEthernet2.0
  no ip address
  ipv6 enable                ↓ 拠点番号を入力
  ipv6 address 2001:db8:1::cafe/64
  ipv6 nd ra enable
  no shutdown
```

・「show running-config」コマンドにより、現在の設定と、ソフトウェアバージョンの確認が可能です。
・保存した設定を確認するときは「show startup-config」コマンドを使用します。

ルーティングテーブルの表示

ルーティングテーブルの表示（show ipv6 route）

```
Router(config)# show ipv6 route
IPv6 Routing Table - 7 entries, unlimited
Codes: C - Connected, L - Local, S - Static
       R - RIPng, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       s - Summary
Timers: Uptime/Age
C      2001:db8::/64 global [0/1]
         via ::, GigaEthernet0.0, 0:49:02/0:00:00
L      2001:db8::/128 global [0/1]
         via ::, GigaEthernet0.0, 0:49:03/0:00:00
L      2001:db8::11/128 global [0/1]
         via ::, GigaEthernet0.0, 0:49:02/0:00:00
C      2001:db8:1::/64 global [0/1]
         via ::, GigaEthernet2.0, 1:06:26/0:00:00
L      2001:db8:1::/128 global [0/1]
         via ::, GigaEthernet2.0, 1:06:27/0:00:00
L      2001:db8:1::cafe/128 global [0/1]
         via ::, GigaEthernet2.0, 1:06:26/0:00:00
S      2001:db8:100::/64 global [1/1]
         via 2001:db8::beef, GigaEthernet0.0, 0:49:03/0:00:00
```

- 「show ipv6 route」コマンドにより、IPv6の経路情報テーブルを表示させることが可能です。
- 目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りが無いかを確認する場合に利用します。

IPv6インターフェース確認

IPv6 インターフェース情報の表示（show ipv6 interface）

```
Router(config)# show ipv6 interface GigaEthernet2.0
Interface GigaEthernet2.0 is up, line protocol is up
Global address(es):
    2001:db8:1::cafe prefixlen 64
    2001:db8:1:: prefixlen 64 anycast
Neighbor discovery variable(s):
    Neighbor cache garbage time 0 seconds
  Router advertisement variable(s):
    Sending RA is enabled
    Max transmit interval 600 seconds
    Min transmit interval 198 seconds
    Reachable time 0 seconds
    Life time 1800 seconds
    Retrans timer 0 milliseconds
    Current hop limit 64 hops
    Managed address configuration flag is off
    Other stateful configuration flag is off
    Prefix is auto-prefix11 address 2001:db8:1:: prefixlen 64
```

・IPv6インターフェースの状態を確認する際に利用します。
装置に設定したプレフィックスやRAで広告する情報も確認出来ます。

Empowered by Innovation

お知らせ

実機教育セミナー

UNIVERGE IXシリーズでは、社内の営業/SE、販売店様向けに実機セミナーを開催しております。

少人数制！（最大10名まで）
機能概要からコマンドまで丁寧に説明！
一人一台の実機を使用することができます！

参加費無料！

提案力強化編（半日教育）
IXシリーズの特徴やお客様の課題に対するソリューションの提案方法などを中心に学習できますので、営業の方にお勧めの新規コースです。IXのウリを説明する【座学】とIX2105のWeb-GUIを使った【演習】に分かれていますので、時間のない方は【座学コースのみ】を受講可能です。

初級編
インターネット接続の設定やインターネットVPNの設定等を体験していただけます。基礎から学べるので、初心者の方でも受講可能です。

応用編（IPsec）
インストラクターによるIPsecの技術概要説明をはじめ、実際にIXルータを使ってのインターネットVPNの構築を体験していただけます。

応用編（OSPF/QoS）
インストラクターによるOSPF/QoSの技術概要説明をはじめ、実際にIXルータを使っての音声/データ統合ネットワークの構築を体験していただけます。

応用編（冗長構成）
IXの特長機能であるネットワークモニタ機能の説明を中心に、ISDNﾊﾞｯｸｱｯﾌﾟやVPNの二重化、VRRPによる機器二重化の設定を体験していただけます。
（本コースのみ最大 8名まで）

■ お申し込みはこちらをご確認ください。
社内 営業/SE向け ： *http://www.cnse.mt.nec.co.jp/#tabs-2*

お知らせ

サンプルコンフィグ作成ツール

サンプルコンフィグを作成するツールを社外サイトに公開しています。

パラメータを入力して…

ボタンを押すだけで

コンフィグが作成できます！

基本設定の確認に是非ご活用ください。

サンプルコンフィグ作成ツール
http://jpn.nec.com/univerge/ix/Support/tool/index.html

お知らせ

技術情報サイトのご案内

製品情報の収集やコンフィグ設計を支援する各種情報を、Webに掲載しています。

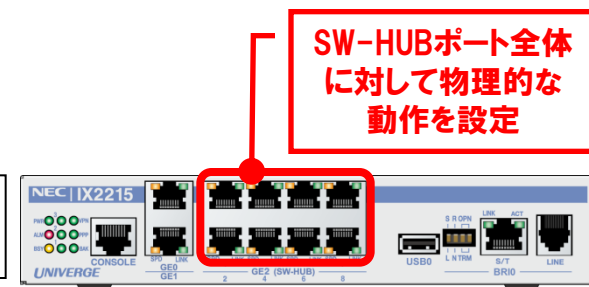
■ ソフトウェアダウンロード
各種マニュアル
製品紹介資料
性能データ
検証レポート
過去Q&A検索 など

■ 仕様一覧
各種マニュアルダウンロード
サンプルコンフィグ作成ツール
FAQ など

LANインタフェースの設定（MDI/MDI-X固定）

LANポートのモード設定（デバイスコンフィグモード）

★SW-HUBポート全体に対して設定する例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# mdi-mdix mdi
```

・LANポートのモード設定
- mdi-mdix [mdi | mdix]：MDI/MDI-X固定設定（speed/duplexともに固定設定時のみ有効）
- exit で上位モードに復帰

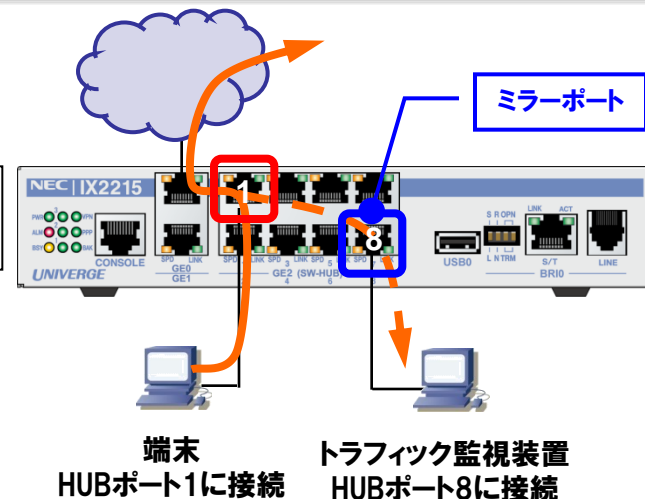
★特定のSW-HUBポートに対して設定する例

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# port 1 mdi-mdix mdi
ROUTER-A(config-GigaEthernet2)# port 8 mdi-mdix mdi
```

LANインタフェースの設定（高機能）

ポートミラーリング設定（デバイスコンフィグモード）

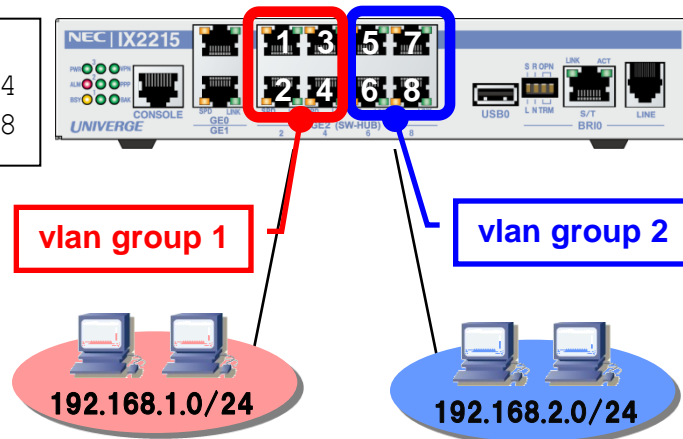
```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# port 1 mirror-port 8 both
```

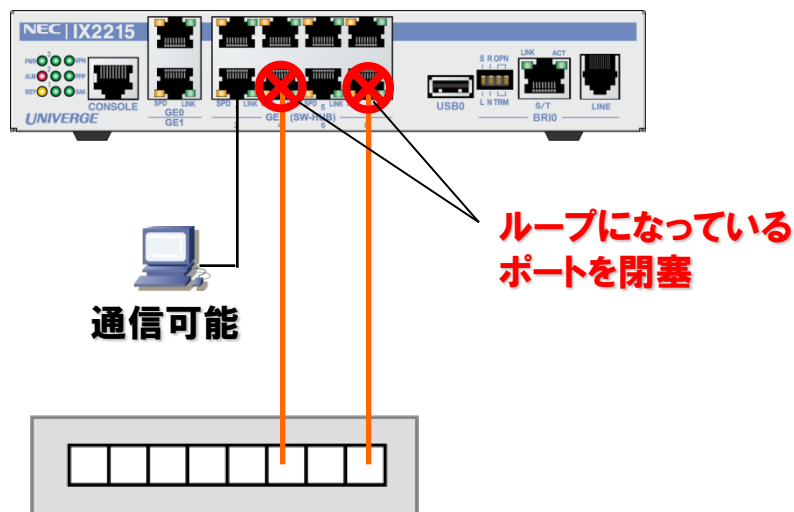
- ポートミラーリングの設定
  - モニタポート（トラフィックを監視するポート）の設定
  - ミラーポート（モニタポートのトラフィックをコピーして送信するポート）の設定
  - モニタするトラフィックの方向設定
    out：送信トラフィックをモニタ　both：送受信するトラフィックをモニタ

ポートVLANの設定（デバイスコンフィグモード）

```
ROUTER-A(config)# device GigaEthernet2
ROUTER-A(config-GigaEthernet2)# vlan-group 1 port 1 2 3 4
ROUTER-A(config-GigaEthernet2)# vlan-group 2 port 5 6 7 8
```

- ポートVLANの設定
  - VLANグループ番号 [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8]
  - ポート番号 [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8]

VLANグループでグループ分けすることで
複数のセグメントを構成することができます。

LANインタフェースの設定（ループ検出）

ループ検出機能（インタフェースコンフィグモード） ※ IX2215のスイッチポートのみ対応

```
ROUTER-A(config)# interface GigaEthernet2.0
ROUTER-A(config-GigaEthernet2.0)# loop-detection enable
```

誤ってケーブルを挿して、ループになっても、他のポートの通信へ影響を与えません。

競合他社 比較一覧（小規模拠点用ルータ）

		IX2105	RTX810	Cisco881	Si-R G100	AR415S
希望小売価格（税別）		81,000円	72,000円	114,000円	79,000円	69,800円
性能（公称値）		最大1.3Gbps	最大1Gbps	不明	最大1.8Gbps	最大197Mbps
IPsec性能（公称値）		最大440Mbps （AES）	最大200Mbps	15Mbps （3DES）	最大440Mbps	最大 96Mbps
FastEthernetポート（10/100）		-	-	1+4 (SW-HUB)	-	1+4 （SW-HUB）
GigabitEthernetポート		1+4 (SW-HUB)	1+4 (SW-HUB)	-	1+4 （SW-HUB）	-
ハードウェア仕様	消費電力	14VA (7W) 以下	最大11W	最大60W	最大15.5W （*5）	最大10.7W
	騒音	0dB（ファンレス）	0dB（ファンレス）	不明	0dB（ファンレス）	0dB（ファンレス）
	環境への配慮	RoHS対応	RoHS対応	不明	不明	RoHS対応
	動作温度条件	0～50℃	0～50℃	0～40℃	0～40℃	0～40℃
設置性		横置き、縦置き、19インチラック (*1)、壁掛け (*2)、マグネット (*3)	横置き、19インチラック (*4) ウォールマウントキット (*4)	横置き、19インチラック (*4)	横置き、縦置き	横置き、壁掛け (*4)、19インチラック (*4)
ブリッジ機能		トランスペアレントブリッジ、IRB、Ethernet over IP、Ethernet over GRE	-	トランスペアレントブリッジ、IRB、L2TPv3	トランスペアレントブリッジ、Ethernet over IP	トランスペアレントブリッジ、L2TP
VLAN		IEEE802.1Q、ポートVLAN (SW-HUB)	IEEE802.1Q、LAN分割	IEEE802.1Q、ポートVLAN（SW-HUB）	IEEE802.1Q、ポートVLAN (SW-HUB)	IEEE802.1Q、ポートVLAN（SW-HUB）
データコネクト対応		○	○	-	-	-
ルーティング (IPv4)	対応方式	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、EIGRP、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4 (*4) ポリシールーティング
	経路数	4096	2000	不明	不明	不明
	OSPFネイバ数	128	10	不明	不明	不明
	OSPF NSSA	○	-	○	○	○
	BGPルートリフレクタ	○	-	○	-	-
	マルチキャスト	PIM-SM, IGMPv1/v2	-	PIM-SM, PIM-DM, PIM-SSM	PIM-SMv2, PIM-DM, IGMPv2	PIM-SM, PIM-DM. IGMPv2

Empowered by Innovation

競合他社 比較一覧(小規模拠点用ルータ)

		IX2105	RTX810	Cisco881	Si-R G100	AR415S
冗長機能	機能	VRRP、 ネットワークモニタ	VRRP、 ICMP Echoによる迂回	VRRP、HSRP、 オブジェクトトラッキング	VRRP、ECMP(static,OSPFv2)、 レイヤー3セッション監視 ・維持機能	VRRP、 Ping ポーリング
	Ping監視先 登録可能数	128	6	不明	不明	不明
QoS		PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、DTC、 ToS/CoS制御、 シェーピング	PQ、CQ、WFQ、LLQ、CBWFQ、 ToS/CoS制御、シェーピング	PQ、WFQ、IPHC、 ToS/CoS制御、 シェーピング	プライオリティーベースルーティング、 COS制御
拡張機能	フィルタ	MACフレームフィルタリング、 IPパケットフィルタリング (静的/動的)	MACフレームフィルタリング、 IPパケットフィルタリング (静的/動的)、URL	MACフレームフィルタリング、 IPパケットフィルタリング (静的/動的)	MACフレームフィルタリング、 IPパケットフィルタリング (静的/動的)、URL	MACフレームフィルタリング、 IPパケットフィルタリング (静的/動的)
VPN	対応方式	IPIP、GRE、IPSec	IPIP、IPsec、PPTP	IPIP、GRE、IPSec	IPIP、IPsec	IPIP(6to4)、GRE、IPsec
	暗号アルゴリズム	DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/192/256bit)
	対地数	128	6	20	100	50
	IKEv2	○	○	○	○	-
	SHA-2	○	○	○	○	-
不正端末アクセス防止, 検疫機能		MACアドレス認証、 IEEE802.1X認証, PC検疫	DHCP端末認証、 Winnyフィルタ	IEEE802.1X認証	MACアドレス認証、 IEEE802.1X認証、 DHCP端末認証	MACアドレス認証, IEEE802.1X認証, アプリケーション検出・遮断
保守機能		SNMP、Syslog、Telnet、SSH、 TFTP、sFlowエージェント、 Web-GUI(保守操作のみ)	SNMP、Syslog、Telnet、TFTP Web-GUI、Luaスクリプト	SNMP、Syslog、Telnet、 TFTP、NetFlow 他	SNMP、Syslog、Telnet、 SSH、FTP、Web管理	SNMP、Syslog、Telnet、 TFTP
ソフトウェア管理機能		プログラムファイル2面管理、 自動バージョンアップ	ファームウェア多重、 Downloadボタン、外部メモリ	-	構成定義2面管理、 外部メモリ	-
自動コンフィグ機能		ゼロコンフィグ(IX2105-Z), 自動コンフィグダウンロード機能	FOMAリモートセットアップ機能	-	-	-
IPv6対応		○ IPv6 Ready Logo Phase.2 (Router,IPsec SGW, IPSec End-Node)取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み

*1: 別売の「19RM-1U2(19インチラックマウントキット)」が必要。*2: 別売の「壁掛けキット」が必要。
*3: 別売の「マグネットセット」が必要。 *4: オプション *5: USBの電力を規格値(2.5W)として加味

2013年9月 当社調べ

Empowered by Innovation

競合他社 比較一覧（オールインワンルータ）

		IX2025	IX2215	RTX1200	Cisco892J	Si-R G200	AR640S
希望小売価格（税別）		115,000円	118,000円	125,000円	128,000円	118,000円	125,000円
性能（公称値）		最大200Mbps	最大2Gbps	最大1Gbps	最大1.8Gbps	最大1.9Gbps	最大750Mbps
IPsec性能（公称値）		最大200Mbps（AES） ※ヘッダ分含む	最大1.3Gbps（AES）	最大200Mbps	200Mbps（3DES）	最大650Mbps	最大339Mbps
FastEthernetポート（10/100）		2+4（SW-HUB）	-	-	1+8（SW-HUB）	-	-
GigabitEthernetポート		-	2+8（SW-HUB）	2+8（SW-HUB）	1	2+8（SW-HUB）	2+4
ISDN対応		1BRI（S/T, U）	1BRI（S/T, U）	1BRI（S/T）	1BRI（S/T）	-	-
無線WAN対応		○ WA1020と連携	○	○	-	○	○
ハードウェア仕様	消費電力	13VA（9W）以下	28VA（18W）以下	最大16W	最大60W	最大29.1W（*5）	最大38W
	騒音	0dB（ファンレス）	0dB（ファンレス）	0dB（ファンレス）	不明（ファン有り）	最大45dB（ファン有り）	不明（ファン有り）
	環境への配慮	RoHS対応	RoHS対応	RoHS対応	不明	不明	RoHS対応
	動作温度条件	0～45℃	0～45℃	0～40℃	0～40℃	0～40℃	0～50℃
設置性		横置き、縦置き（*1）、 19インチラック（*2）、 二段重ね（*3）	横置き、縦置き（*1）、 19インチラック（*2）、 二段重ね（*3）	横置き、19インチラック（*4） ウォールマウントキット（*4）	横置き、 19インチラック（*4）	横置き、 ラック搭載機構（*4）	横置き、 19インチラック（*4）、 壁掛け（*4）、マグネット（*4）
ブリッジ機能		トランスペアレントブリッジ、 IRB、Ethernet over IP 、 Ethernet over GRE	トランスペアレントブリッジ、 IRB、Ethernet over IP 、 Ethernet over GRE	L2TPv3	トランスペアレントブリッジ、 IRB、L2TPv3	トランスペアレントブリッジ、 Ethernet over IP	トランスペアレントブリッジ、 L2TP
VLAN		IEEE802.1Q、 ポートVLAN（SW-HUB）	IEEE802.1Q、 ポートVLAN（SW-HUB）	IEEE802.1Q、 LAN分割	IEEE802.1Q、 ポートVLAN（SW-HUB）	IEEE802.1Q、 ポートVLAN（SW-HUB）	IEEE802.1Q、 ポートVLAN（SW-HUB）
ISDNバックアップ		○（INS64）	○（INS64）	○（INS64）	○（INS64）	-	-
データコネクト対応		○	○	○	-	-	-
ルーティング（IPv4）	対応方式	RIP/RIPv2、OSPF、BGP4、 ポリシールーティング	RIP/RIPv2、OSPF、BGP4、 ポリシールーティング	RIP/RIPv2、OSPF、BGP4、 ポリシールーティング	RIP/RIPv2、OSPF、BGP4、 EIGRP、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、 ポリシールーティング	RIP/RIPv2
	経路数	4096	4096	10000	不明	不明	不明
	OSPFネイバ数	128	128	30	不明	不明	-
	OSPF NSSA	○	○	-	○	○	-
	BGPルートリフレクタ	○	○	-	○	-	-
	マルチキャスト	PIM-SM, IGMPv1/v2	PIM-SM, IGMPv1/v2	-	PIM-SM, PIM-DM, PIM-SSM	PIM-SMv2, PIM-DM, IGMPv2	-

競合他社 比較一覧（オールインワンルータ）

		IX2025	IX2215	RTX1200	Cisco892J	Si-R G200	AR640S
冗長機能	機能	VRRP、 ネットワークモニタ	VRRP、 ネットワークモニタ	VRRP、 ICMP Echoによる迂回	VRRP、HSRP、 オブジェクトトラッキング	VRRP、 ECMP（static,OSPFv2）、 レイヤー3セッション監視 ・維持機能	VRRP、 Ping ポーリング
	Ping監視先 登録可能数	128	128	100	不明	不明	不明
QoS		PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、DTC、 ToS/CoS制御、 シェーピング	PQ、CQ、WFQ、LLQ、CBWFQ、 ToS/CoS制御、シェーピング	PQ、WFQ、IPHC、 ToS/CoS制御、 シェーピング	-
拡張機能	フィルタ	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）、URL	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）、URL	MACフレームフィルタリング、 IPパケットフィルタリング （静的/動的）
VPN	対応方式	IPIP、GRE、IPSec	IPIP、GRE、IPSec	IPIP、IPSec、PPTP	IPIP、GRE、IPSec	IPIP、IPsec	IPsec
	暗号アルゴリズム	DES, 3DES AES（128/192/256bit）	DES, 3DES AES（128/192/256bit）	DES, 3DES, AES（128/256bit）	DES, 3DES AES（128/192/256bit）	DES, 3DES AES（128/192/256bit）	DES, 3DES AES（128/192/256bit）
	対地数	128	128	100	50	100	100
	IKEv2	○	○	○	○	○	○
	SHA-2	○（*6）	○	○	○	○	-
不正端末アクセス防止, 検疫機能		MACアドレス認証、 IEEE802.1X認証, PC検疫	MACアドレス認証、 IEEE802.1X認証, PC検疫	DHCP端末認証、 Winnyフィルタ	IEEE802.1X認証	MACアドレス認証、 IEEE802.1X認証、 DHCP端末認証	アプリケーション検出・遮断
保守機能		SNMP、Syslog、Telnet、SSH、 TFTP 、sFlowエージェント、 Web-GUI（保守操作のみ）	SNMP、Syslog、Telnet、SSH、 TFTP 、sFlowエージェント、Web- GUI（保守操作のみ）	SNMP、Syslog、Telnet、TFTP Web-GUI、Luaスクリプト	SNMP、Syslog、Telnet、 TFTP、 NetFlow 他	SNMP、Syslog、Telnet、 SSH、FTP、Web管理	SNMP、Syslog、Telnet、TFTP
ソフトウェア管理機能		プログラムファイル2面管理、 自動バージョンアップ	プログラムファイル2面管理、 自動バージョンアップ	ファームウェア多重、 Downloadボタン、外部メモリ	-	構成定義2面管理、 外部メモリ	-
自動コンフィグ機能		ゼロコンフィグ（IX2025-Z）， 自動コンフィグダウンロード機能	ゼロコンフィグ（IX2215-Z）， 自動コンフィグダウンロード機能	FOMAリモートセットアップ機能	-	-	-
IPv6対応		○ IPv6 Ready Logo Phase.2 （Router,IPsec SGW, IPSec End-Node）取得済み	○ IPv6 Ready Logo Phase.2 （Router,IPsec SGW, IPSec End-Node）取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み

*1: 別売の「スタンドキット」が必要。 *2: 別売の「19RM-1U2（19インチラックマウントキット）」が必要。
*3: 別売の「ジョイントキット」が必要。 *4: オプション
*5: USBの電力を規格値（2.5W）として加味 *6: ソフト処理

2013年9月 当社調べ

競合他社 比較一覧（センタールータ）

		IX3010	IX3110	RTX3500	RTX5000	Cisco2901	Si-R570
希望小売価格（税別）		338,000円	798,000円	498,000円	798,000円	329,000円	900,000円
性能（公称値）		最大850Mbps	最大2.6Gbps	最大4Gbps	最大4Gbps	不明	最大500Mbps
IPsec性能（公称値）		最大260Mbps（AES）（*1）	最大920Mbps（AES）	最大1.5Gbps（AES）	最大2.0Gbps（AES）	170Mbps（AES）	最大500Mbps（3DES）
FastEthernetポート（10/100）		2（最大6）	-	-	-	0（増設可）（*6）	4（最大10）（*6）
GigabitEthernetポート		0（最大2）	4（*5）	2+4（SW-HUB）+4（SW-HUB）	2+4（SW-HUB）+4（SW-HUB）	2（増設可）（*6）	0（最大2）（*6）
WANポート	BRI	0（最大8）（*2）	-	0（最大8）（*6）	0（最大8）（*6）	0（増設可）（*6）	0（最大2）（*6）
	T1	0（最大2）（*3）	-	0（最大1）（*6）	0（最大1）（*6）	0（増設可）（*6）	0（最大2）（*6）
ハードウェア仕様	消費電力	95VA（60W）以下	65VA（40W）以下	最大37W	最大38W	150W	最大70W
	騒音	50dB以下	50dB以下	不明	不明	最大61dB	50dB
	電源冗長	内蔵型（*4）	内蔵型（*4）	-	-	-	内蔵型（*6）
	環境への配慮	RoHS対応	RoHS対応	RoHS対応	RoHS対応	不明	-
設置性		横置き、19インチラック	横置き、19インチラック	横置き、19インチラック	横置き、19インチラック	横置き、19インチラック	横置き、19インチラック
ブリッジ機能		トランスペアレントブリッジ、IRB、Ethernet over IP 、Ethernet over GRE	トランスペアレントブリッジ、IRB、Ethernet over IP 、Ethernet over GRE	-	-	トランスペアレントブリッジ、IRB、L2TPv3	トランスペアレントブリッジ、IRB、Ethernet over IP
VLAN		IEEE802.1Q、ポートVLAN（SW-HUB）	IEEE802.1Q	IEEE802.1Q	IEEE802.1Q	IEEE802.1Q	IEEE802.1Q
ISDNバックアップ		○（INS64、INS1500）（*1）	-	○（INS64、INS1500）	○（INS64、INS1500）	○（INS64、INS1500）	○（INS64、INS1500）
データコネクト対応		○	○	○	○	-	-
ルーティング（IPv4）	対応方式	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、EIGRP、BGP4、ポリシールーティング	RIP/RIPv2、OSPF、BGP4、ポリシールーティング
	経路数	8192	20000	20000	60000	メモリ依存	10000
	OSPFネイバ数	128	128	60	60	不明	50
	OSPF NSSA	○	○	-	-	○	○
	BGPルートリフレクタ	○	○	-	-	○	-
	マルチキャスト	PIM-SM, IGMPv1/v2	PIM-SM 、IGMPv1/v2	-	-	PIM-SM, PIM-DM, PIM-SSM	PIM-SM, PIM-DM, IGMPv2

競合他社 比較一覧（センタールータ）

		IX3010	IX3110	RTX3500	RTX5000	Cisco2901	Si-R570
冗長機能	機能	VRRP（*1）、ネットワークモニタ	VRRP、ネットワークモニタ	VRRP、ICMP Echoによる迂回	VRRP、ICMP Echoによる迂回	VRRP、HSRP、オブジェクトトラッキング	VRRP、レイヤー3セッション監視機能
	Ping監視先登録可能数	512	1024	1000	3000	不明	不明
QoS		PQ、CBQ、LLQ、ToS/CoS制御、シェーピング	PQ、CBQ、LLQ、ToS/CoS制御、シェーピング	PQ、CBQ、ToS/CoS制御、シェーピング、適応型QoS	PQ、CBQ、ToS/CoS制御、シェーピング、適応型QoS	PQ、CQ、WFQ、LLQ、CBWFQ、ToS/CoS制御、シェーピング	WFQ、ToS/CoS制御、シェーピング
拡張機能	フィルタ	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）、URL	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）、URL	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）	MACフレームフィルタリング、IPパケットフィルタリング（静的/動的）、URL
VPN	対応方式	IPIP、GRE、IPSec（*1）	IPIP、GRE、IPSec	IPIP、IPSec	IPIP、IPSec	IPIP、GRE、IPSec	IPIP、IPSec
	暗号アルゴリズム	DES, 3DES AES（128/192/256bit）	DES, 3DES, AES（128/192/256bit）	DES, 3DES, AES（128/256bit）	DES, 3DES, AES（128/256bit）	DES, 3DES, AES（128/192/256bit）	DES, 3DES, AES（128/192/256bit）
	対地数	512	1024	1000	3000	不明	1000
	IKEv2	○	○	○	○	○	○
	SHA-2	○（*7）	○（*7）	○	○	○	-
不正端末アクセス防止, 検疫機能		MACアドレス認証、IEEE802.1X認証, PC検疫	MACアドレス認証、IEEE802.1X認証, PC検疫	DHCP端末認証、Winnyフィルタ	DHCP端末認証、Winnyフィルタ	IEEE802.1X認証	MACアドレス認証、IEEE802.1X認証、DHCP端末認証
保守機能		SNMP、Syslog、Telnet、SSH、TFTP 、sFlowエージェント、Web-GUI（保守操作のみ）	SNMP、Syslog、Telnet、SSH TFTP 、sFlowエージェント、Web-GUI（保守操作のみ）	SNMP、Syslog、Telnet、SSH、TFTP	SNMP、Syslog、Telnet、SSH、TFTP	SNMP、Syslog、Telnet、TFTP、 NetFlow 他	SNMP、Syslog、Telnet、SSH、FTP、Web管理
ソフトウェア管理機能		プログラムファイル2面管理、自動バージョンアップ	プログラムファイル2面管理、自動バージョンアップ	ファームウェア多重	ファームウェア多重	-	-
自動コンフィグ機能		自動コンフィグダウンロード機能	ゼロコンフィグ（IX3110-Z）, 自動コンフィグダウンロード機能	FOMAリモートセットアップ機能	FOMAリモートセットアップ機能	-	-
IPv6対応		○ IPv6 Ready Logo Phase.2（Router,IPsec SGW, IPSec End-Node）取得済み	○ IPv6 Ready Logo Phase.2（Router,IPsec SGW, IPSec End-Node）取得済み	- Logo未取得	- Logo未取得	○ IPv6 Ready Logo Phase.2 取得済み	○ IPv6 Ready Logo Phase.2 取得済み

2013年9月 当社調べ

*1: IX3010の「IPsec高速化」、「VRRP」、「ISDN」を使用する場合、別売のオプションソフトウェアが必要。
*2: 別売の「4BRI-STカード」を2枚実装時。
*3: 別売の「T1カード」を2枚実装時。　*4: 別売の「冗長AC電源キット」が必要。
*5: 各4ポートは「10/100/1000BASE-T」もしくは「1000BASE-SX/LX」の選択が可能。1000BASE-SX/LXで使用する場合、別売の「SFPモジュール」が必要。
*6:オプション　*7:IX3010:ソフト処理、IX3110:SHA-256のみハード処理